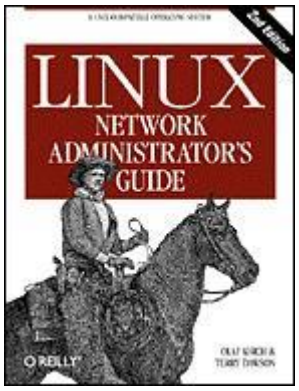
LINUX

REDE

ADMINISTRADOR DE GUIA



por Olaf Kirch e Terry Dawson

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Copyright © 1993 Olaf Kirch
Copyright © 2000 Terry Dawson
Direitos autorais na O'Reilly versão impressa © 2000 O'Reilly & Associates

Publicação para a Internet por Albrecht Jan
jan@jan-albrecht.de

Um versão atual deste documento pode ser baixado em http://www.jan-albrecht.de/nag/nag.ZIP

Esta é a versão original do documento, que foi lançado.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

PREFÁCIO 12
POBJECTIVO E AUDIENCE PARA THIS BOOK 12
SONTES DE IINFORMAÇÃO 13
Documentação disponível via FTP *14*
Documentação disponível via WWW *14*
Documentação disponível comercialmente *14*
Linux Journal e da revista Linux *15*
Usenet Newsgroups Linux *15*
Listas de discussão Linux *15*
Suporte Online Linux *16*
Grupos de usuários Linux *16*
Obter Linux *16*
FILE SISTEMA STANDARDS 17
SPADRÃO LInux BASE 17
ABOUT THIS BOOK 18
THE OESIGNAÇÃO PMPRESSO VErsão 19
OANORÂMICA 19
CONVENÇÕES USED EM THIS BOOK 20
SUBMITTING CUDANÇAS 21
AGRADECIMENTOS 21
O Hall da Fama *22*
CAPÍTULO 1 - Introdução às Redes 23
HISTÓRIA 23
N TCP / IPEDES 23
Introdução às redes TCP / IP *24*
Ethernets *25*
Outros tipos de Hardware *26*
O Protocolo de Internet *27*
IP sobre linhas seriais *28*
O Transmission Control Protocol *28*
O User Datagram Protocol *29*
Mais de Portos *29*
A Biblioteca Socket *29*
UUCP NEDES 30
LInux NETWORKING 30
Listras diferentes de desenvolvimento *31*
Onde obter o código *31*
MANTER YNOSSA SISTEMA 32
Sistema de Segurança *32*
CAPÍTULO 2 - Questões de rede TCP / IP 34
NETWORKING INTERFACES 34
A IPDDRESSES 34
AENDEREÇO RESOLUÇÃO 36
IP REXCURSÃO 36
Redes IP *36*
Subredes *37*
Gateways *37*
A tabela de roteamento *39*
Metric Valores *40*
THE INTERNET CCONTROLO MENSAGEM PROTOCOLO 40
RESOLVING HOST NAMES 41
CAPÍTULO 3 - Configurando o hardware de rede 42
KERNEL CONFIGURAÇÃO 44
Opções do Kernel do Linux 2.0 e superior *44*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A TNOSSO DE LInux NREDE DEVICES 48
ETHERNET INSTALAÇÃO 49
Detecção automática Ethernet 49
THE PLIP DRIO 51
THE PPP E SLIP DRIOS 52
OLÁ NREDE TIPOS 52
CAPÍTULO 4 - configurar o hardware SERIAL 53
COMUNICAÇÕES SMPRESSORA PARA MODEM LTINTAS 53
IINTRODUÇÃO AO SErial DEVICES 53
ACESSO SErial DEVICES 54
O dispositivo serial Arquivos Especiais 55
SErial HARDWARE 55
UCANTO DO CONFIGURAÇÃO UTilidades 56
O comando setserial 56
O comando stty 58
SErial DEVICES eo login: PRompt 60
Configurando o Daemon mgetty 60
CAPÍTULO 5 - Configurando o TCP / IP 63
MO ONTAGEM /PROC FILESYSTEM 63
INSTALAÇÃO DO BINARIES 63
SDEFINIR OS HOSTNAME 64
ASSIGNING A IPDDRESSES 64
CRIAÇÃO SUBNETS 65
WRiting hosts e redes FILES 65
INterface CONFIGURAÇÃO PARA IP 66
A interface loopback 67
Interfaces Ethernet 68
Roteamento através de um gateway 69
Configurando um Gateway 70
A Interface PLIP 70
As interfaces SLIP e PPP 71
A interface dummy 71
Alias IP 71
ALL ABOUT ifconfig 72
THE NETSTAT COmmand 74
Exibindo a tabela de roteamento 74
Resultados de Estatísticas Interface 75
Exibindo Conexões 75
CA verificação da T ARPABLES 76
CAPÍTULO 6 - SERVIÇO DE NOME E CONFIGURAÇÃO DE RESOLVER 78
THE RESOLVER LIBRARY 78
O host.conf Arquivo 78
O arquivo nsswitch.conf 80
Pesquisas Server Configurando Nome Usando resolv.conf 81
Robustez Resolver 82
HOW DNS WOrks 83
Nome pesquisas com o DNS 84
Tipos de servidores de nomes 85
O banco de dados DNS 85
Pesquisas Reversas 87
RUNNING NOMEADO 88
O arquivo named.boot 88
O BIND 8 host.conf Arquivo 90
O DNS arquivos de banco de dados 91
Caching-somente o nome de configuração 93
Escrevendo o arquivos Master 94

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Verificando a Instalação de Servidor de Nomes *96*
Outras ferramentas úteis *98*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

CAPÍTULO 7 - IP LINE SÉRIE 99
GGERAL REQUISITOS 99
O SLIPFUNCIONAMENTO 99
DEALING COM PRIVATE IP NEDES 101
USING DIP 101
Um script de exemplo 102
Um mergulho Referência 103
RUNNING EM SERVER MODE 105
Capítulo 8 - O Protocolo Ponto-a-POINT 108
PPP ON LINUX 108
RUNNING DPF 109
USING OPÇÕES FILES 110
USING DE CHAT AUTOMATE DIALING 110
IP CONFIGURAÇÃO OPÇÕES 112
Escolha dos endereços IP 112
Roteamento Através de um link PPP 113
LTINTA CCONTROLO OPÇÕES 114
GGERAL SSEGURANÇA CCONSIDERAÇÕES 115
AUTENTICAÇÃO COM PPP 116
PAP Versus CHAP 116
Os segredos CHAP Arquivo 117
O PAP Arquivo Segredos 117
DEBUGGING YNOSSA PPP SETUP 118
MORE AAVANÇADO PPP CONFIGURATIONS 118
Servidor PPP 118
Discagem por demanda 120
Discagem persistente 120
CAPÍTULO 9 - TCP / IP FIREWALL 122
MÉTODOS DE ATTACK 122
WHAT IS A FIREWALL? 123
WHAT IS IP FILTERING? 124
SIXAR UP LINUX PARA FIREWALLING 125
Kernel configurado com IP Firewall 125
O utilitário ipfwadm 126
O utilitário ipchains 126
O utilitário iptables 126
TETRP WAYS WE CAN DO FILTERING 126
OI nédito IP FIREWALL (2,0 KERNELS) 127
Usando ipfwadm 128
Um exemplo mais complexo 130
Resumo dos argumentos ipfwadm 131
IP FIREWALL CHains (2,2 KERNELS) 133
Usando ipchains 134
ipchains Sintaxe do Comando 134
Nosso exemplo ingênuo Revisited 137
Listagem de nossas regras ipchains 137
Fazendo bom uso das Correntes 138
NE ETFILTER T IPABLES (2,4 KERNELS) 141
Compatibilidade com versões anteriores com ipfwadm e ipchains 143
Usando o iptables 143
Nosso exemplo ingênuo Revisited, uma vez mais 147
TOS BTI MANIPULATION 147
Definir o TOS ipfwadm Bits Usando ipchains ou 148
Estabelecer os bits TOS Usando o iptables 148
TA interessantes FIREWALL CONFIGURAÇÃO 149
A SAMPLA FIREWALL CONFIGURAÇÃO 150

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

CAPÍTULO 10 - CONTABILIDADE IP 157
CO ONFIGURAR KERNEL PARA A IPCONTABILIDADE..... 157

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

CONFIGURAR A IPCONTABILIDADE 157
Contabilidade por Endereço 158
Contabilidade pela porta de serviço 159
Contabilidade de datagramas ICMP 161
Contabilidade pelo Protocolo 161
USING A IPCONTABILIDADE RESULTADOS 162
Listagem de Dados Contábeis com ipfwadm 162
Listagem de Dados Contábeis com ipchains 162
Listagem de Dados Contábeis com iptables 162
REINICIALIZAR O COUNTERS 163
FO LUSHING RULESET 163
PAssive COLLECTION DE ACONTABILIDADE DATA 163
CAPÍTULO 11 - MASQUERADE E Network Address Translation 165
SIDE EFEITOS E FRinge BENEFÍCIOS 166
CO ONFIGURAR KERNEL PARA IP MASQUERADE 166
CONFIGURAR IP MASQUERADE 167
Definir parâmetros de tempo para a IP Masquerade 169
HANDLING NAME SErver LOOKUPS 169
MORE ABOUT NREDE AENDEREÇO TRADUÇÃO 169
CAPÍTULO 12 - RECURSOS importante rede 171
THE INETD SUper SErver 171
THE TCPD ACESSO CCONTROLO FACILITY 173
THE SSERVIÇOS E PROTOCOLOS FILES 174
RFotografar PROCEDIMENTO CALL 175
CONFIGURAR RFotografar LE ogin EXECUÇÃO 176
Desativar o r; Comandos 176
Instalando e Configurando ssh 177
CAPÍTULO 13 - SISTEMA DE INFORMAÇÃO DE REDE 182
GIxar ACQUAINTED COM NIS 182
NIS VERSUS NIS + ... 184
THE CResiliente SIDE DE NIS 184
RUNNING AN NEI SErver 185
NEI SErver SSEGURANÇA 186
SIxar UP AN NIS CResiliente COM GNU LIBC 186
CO SCOLHER RDIREITO MAPS 188
UCANTO DO passwd e grupo MAPS 189
USING NIS COM SHadow SPOIO 190
Capítulo 14 - A Network File System 192
PREPARAÇÃO NFS 193
MONTAGEM AN NFS VOLUME 193
THE NFS DAEMONS 194
TQue exporta FILE 195
KERNEL-BAsed NFSV2 SErver SPOIO 196
KERNEL-BAsed NFSV3 SErver SPOIO 197
CAPÍTULO 15 - IPX eo sistema de arquivos NCP 198
XErox, NOVELL, E HISTÓRIA 198
IPX E LInux 199
Suporte Caldera 199
Mais sobre Suporte NDS 199
CO ONFIGURAR KERNEL PARA IPX E NCPFS 199
CONFIGURAR IPX INTERFACES 200
Dispositivos de rede de suporte IPX 200
Configuração IPX Tools Interface 200
O ipx_configure Comando 200
O Comando ipx_interface 201
CONFIGURAR AN IPX REXTERIOR 202

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Estático roteamento IPX usando o comando ipx_route *202*
Redes e Roteamento IPX interno *203*
MA ONTAGEM RFotografar NETWSÃO VOLUME..... . 205
Um exemplo simples ncpmount *205*
O Comando ncpmount em detalhe *205*
Escondendo a sua senha do NetWare Login *207*
Um exemplo mais complexo ncpmount *207*
EXPLORING SOME DO OLÁ T IPXOOLS..... 207
Lista de servidores *207*
Enviar mensagens para NetWare Usuários *208*
Navegação e manipulando dados Bindery *208*
PIMPRESSÃO PARA A NETWSÃO PRINT QUEUE 209
Usando nprint com a Line Printer Daemon *210*
Gestão de filas de impressão *211*
NETWSÃO SErver EFormulação 211
CAPÍTULO 16 - GESTÃO DE TAYLOR UUCP 212
T UUCPE RANSFERS RFotografar EXECUÇÃO 213
O funcionamento interno do uucico *213*
uucico Opções de linha de comando *214*
UUCP CONFIGURAÇÃO FILES 215
Uma introdução suave para Taylor UUCP *215*
O UUCP Precisa Saber *217*
Naming Site *217*
Arquivos de configuração Taylor *218*
Geral Configuração de opções usando o arquivo de configuração *218*
How to Tell UUCP sobre outros sistemas usando o arquivo sys *218*
Identificar dispositivos acessíveis através da porta Arquivo *222*
Como discar um número usando o botão Arquivo *223*
UUCP sobre TCP *223*
Usando uma conexão direta *224*
CONTROLLING AACESSO AO UUCP FEATURES 224
Execução de Comandos *224*
Transferência de Arquivos *225*
Encaminhamento *225*
SIxar UP YNOSSA SISTEMA DE DIALING IN..... 226
Fornecer Contas UUCP *226*
Protegendo-se Contra Trapaceiros *227*
Seja Paranoid: Verifica chamada seqüência *227*
UUCP Anónimo *228*
UUCP LOW-LNÍVEL PROTOCOLOS 228
Visão Geral do Protocolo *228*
Ajustando o Protocolo de Transmissão *229*
Seleção de protocolos específicos *229*
TRESOLUÇÃO DE PROBLEMAS 230
Mantém uucico Dizer "Wrong Time to Call "..... *230*
uucico reclama que o site já está bloqueado *230*
Você pode se conectar ao site remoto, mas o bate-papo script falhar *230*
Seu modem não disca *231*
Seu modem tenta discar, mas não sai *231*
Autenticação for bem sucedida, mas a falha de handshake *231*
LOG FE ILES DEBUGGING 231
CAPÍTULO 17 - CORREIO ELETRÔNICO 233
WHAT IS A MAIL MENSAGEM?..... 233
HOW IS MAIL DELIVERED? 235
EMAIL ADDRESSES..... 236
RFC 822 236

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Obsoleto Formatos Mail *236*
Misturando diferentes formatos de correio *237*
HOW DOES MAIL REXCURSÃO WORK?..... 237
Mail Roteamento na Internet *237*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Mail roteamento no Mundo UUCP 238
Misturando UUCP e RFC-822 239
CONFIGURAR ELM 241
Opções globais elm 241
Conjuntos de caracteres Nacional 241
CAPÍTULO 18 - SENDMAIL 243
IINTRODUÇÃO AO SENDMAIL 243
INSTALAR SENDMAIL 243
OANORÂMICA DE CONFIGURAÇÃO FILES 244
TSENDMAIL HE.CF e Sendmail.MC FILES 244
Dois arquivos de exemplo sendmail.mc 244
Normalmente usado Parâmetros sendmail.mc 245
GENERATING sendmail a.CF FILE 248
IE NTERPRETING WRiting REWRITE RREGRAS 248
sendmail.cf R e S Comandos 248
Algumas definições úteis Macro 248
O lado esquerdo 249
O lado direito 249
Um exemplo de padrão simples regra 250
Semântica Ruleset 250
CONFIGURAR SENDMAIL OPÇÕES 252
SOME USEFUL SENDMAIL CONFIGURATIONS 253
Confiando usuário definir o campo From: 253
Gerenciando Alias Mail 253
Usando um host inteligente 254
Gerenciando e-mails indesejados ou não solicitados (spam) 255
Configurando Email Virtual Hosting 257
TTeressante YNOSSA CONFIGURAÇÃO 258
RUNNING SENDMAIL 261
TIPS e TRicks 261
Gerenciando o spool de email 262
Forçando um host remoto para o seu processo fila de correio 262
Análise Estatística Mail 262
CAPÍTULO 19 - COMO EXIM EM SERVIÇO 265
RUNNING EXIM 265
IF YNOSSA MAIL DOESN»T GET THrough 266
COMPILING EXIM 267
MAIL DELIVERY MODES 267
MISCELLANEOUS CONFIG OPÇÕES 268
MENSAGEM REXcursão e DELIVERY 269
Roteamento de mensagens 269
Entrega de mensagens para endereços locais 269
Alias Arquivos 270
Listas de 271
PROTEGENDO AGainst MAIL SPAM 272
UUCP SETUP 272
CAPÍTULO 20 - NetNews 274
USenet HISTÓRIA 274
WHAT IS USenet, ANYWAY? 274
HOW DOES USenet HANDLE NEWS? 275
CAPÍTULO 21 - NOTÍCIAS C 278
DELIVERING NEWS 278
INSTALAÇÃO 279
THE SYS FILE 280
THE ACTIVO FILE 283
AARTIGO BDAPTAR 283

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

EXPIRING NEWS 285

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

MISCELLANEOUS FILES 287
CCONTROLO MENSAGENS 288
O cancelamento Mensagem 288
newgroup e rmgroup 288
O checkgroups Mensagem 288
sendsys, versão e senduuname 289
C NEWS EM UM E NFSMBIENTE 290
MANUTENÇÃO TE OOLS TSOLICITA 290
CAPÍTULO 22 - NNTP eo daemon nntpd 292
THE NNTP PROTOCOLO 293
Conectando ao servidor de notícias 293
Empurrando um artigo de notícia para um servidor 293
Mudar para Modo nnrp Reader 294
Listagem de Grupos disponíveis 295
Listagem de grupos do Active 295
Publicar um artigo 295
Listagem de artigos Novos 296
Selecionando um grupo em que a Operação 296
Listagem de artigos em um grupo 296
Recuperando um cabeçalho Apenas artigo 296
Recuperando um corpo apenas o artigo 297
Lendo um artigo de um grupo 297
INSTALAÇÃO DO NNTP SErver 298
RESTRICTING A NNTPCESSO 298
A NNTPUTORIZAÇÃO 299
Nntpd INTERACTION COM C NEWS 299
CAPÍTULO 23 - notícias da Internet 301
SOME Inn INTERNALS 301
NE EWSREADERS DCI 303
INSTALAR DCI 303
CONFIGURAR DCI: O BASIC SETUP 303
DCI CONFIGURAÇÃO FILES 304
Os parâmetros globais 304
Configurando Newsgroups 305
Configurando Newsfeeds 306
Controlando o acesso Newsreader 309
Vencer Notícias 311
Manipulação de mensagens de controle 312
RUNNING DCI 314
MANAGING DCI: THE CTLINND COmmand 315
Adicionar um novo grupo 315
Alterar um grupo 315
Remover um grupo de 316
Renumerar um Grupo 316
Permitir / Bloquear Newsreaders 316
Rejeitar Newsfeed Conexões 316
Permitir conexões Newsfeed 317
Desative o servidor Notícias 317
Reinicie o servidor de notícias 317
Tela de status de um Newsfeed 317
Largar um Newsfeed 317
Comece um Newsfeed 318
Cancelar um artigo 318
CAPÍTULO 24 - CONFIGURAÇÃO NewsReader 319
TIN CONFIGURAÇÃO 319
TRN CONFIGURAÇÃO 320

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

NN CONFIGURAÇÃO..... 320
APÊNDICE A 322

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

EXEMPLO NREDE: THE VIRTUAL BREWERY 322
CO ONECTANDO VIRTUAL SUBSIDIARY NREDE..... 322
APÊNDICE B - configurações de cabo ÚTEIS 323
A P PLIPARALLEL CABLE 323
A SErial NULL MODEM CABLE 323
APÊNDICE C - INFORMAÇÕES DE DIREITOS AUTORAIS 325
PREAMBLE 325
AE PPLICABILITY DEFINIÇÕES 325
VERBATIM COPYING 326
COPYING EM QUANTIDADE 326
MODIFICAÇÕES 327
COMBINING DOCUMENTOS 328
COLLECTIONS DE DOCUMENTOS..... 328
AGGREGATION COM INDEPENDENTES WOrks..... 328
TRADUÇÃO..... 329
TNCERRAMENTO 329
FFUTURO REVISIONS DESTE LICENSE 329
APÊNDICE D 330

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Prefácio

A Internet é hoje um termo familiar em muitos países. Com as pessoas de outra forma grave começando a joyride
ao longo da Supervia da Informação, redes de computadores parece estar se movendo em direção ao status de aparelhos de TV e fornos de microondas. A Internet tem invulgarmente alta cobertura da mídia, e majores das ciências sociais são descendentes de newsgroups, ambientes de realidade virtual on-line ea Web para realizar pesquisas na Internet "nova
Cultura. "

Claro, a rede tem sido em torno de um longo tempo. A conexão de computadores para formar redes de área local tem
sido uma prática comum, mesmo em pequenas instalações, e assim ter as ligações de longa distância utilizando linhas de transmissão previstas
por empresas de telecomunicações. Um conglomerado de rápido crescimento das redes em todo o mundo, no entanto,
feita juntando a aldeia global uma opção perfeitamente razoável até mesmo para as pequenas organizações sem fins lucrativos das empresas privadas
usuários de computador. Configurando um host da Internet com correio e notícias oferece recursos de discagem e acesso RDIS tecnologias se tornem acessíveis, e com o advento do DSL (Digital Subscriber Line) e Cable Modem vai duvidar-
lessly continue esta tendência.

Falando sobre redes de computadores, muitas vezes significa falar sobre o Unix. Claro, o Unix não é apenas a sua
sistema com capacidades de rede, nem vai continuar a ser um favorito para sempre, mas foi no ramo de redes de
ness por um longo tempo, e certamente irá continuar a ser por algum tempo para vir.

O que faz Unix particularmente interessante para usuários privados é que tem havido muita atividade para trazer Unix livre como sistemas operacionais para PC, como o 386BSD, FreeBSD e Linux.

Linux é uma distribuição livre clones do Unix para computadores pessoais. Ele atualmente roda em uma variedade de máquinas

que
inclui a família de processadores Intel, mas também da Motorola 680x0, como o Commodore Amiga e
Apple Macintosh, Sun SPARC e máquinas Ultra SPARC; Compaq Alphas, MIPS, PowerPC, como a nova
geração da Apple Macintosh, e StrongARM, como o rebel.com Netwinder e máquinas 3Com Palm.
Linux foi portado para algumas plataformas relativamente obscuros, como a Fujitsu AP-1000 e o IBM System 3 / 90.
Portes para outras arquiteturas interessantes estão actualmente em curso nos laboratórios de desenvolvedores, ea busca para mover Linux
no espaço controlador embutido promete sucesso.

Linux foi desenvolvido por uma equipe de voluntários em toda a Internet. O projeto foi iniciado em 1990 por Linus
Torvalds, um estudante universitário finlandês, como um projeto de curso de sistemas operacionais. Desde aquela época, o Linux tem neve
enrolado em um clone do Unix completo capaz de correr aplicações tão diversas como a simulação e modelagem
programas, processadores de texto, sistemas de reconhecimento de voz, navegadores da World Wide Web, e uma horda de outros soft-
ware, incluindo uma variedade de excelentes jogos. Uma grande quantidade de hardware é suportado e Linux contém um com-
implementação completo de rede TCP / IP, incluindo SLIP, PPP, firewalls, uma implementação IPX completo, e
muitos recursos e alguns protocolos não encontradas em nenhum outro sistema operacional. Linux é poderoso, rápido e gratuito, e
sua popularidade no mundo para além do Internet está crescendo rapidamente.

O sistema operacional Linux em si é coberta pela GNU General Public License, a licença do mesmo autor
usada por um software desenvolvido pela Free Software Foundation. Esta licença permite que qualquer um redistribuir ou mod-
verificam o software (gratuito ou com um lucro), contanto que todas as modificações e distribuições livremente estão distribuindo
capazes também. O "software livre" se refere à liberdade de aplicação, não a liberdade de custo.

Objetivo e público alvo deste livro

Este livro foi escrito para fornecer uma referência única para administração de rede em um ambiente Linux. Comece-
parceiros e usuários experientes deveriam encontrar a informação de que necessitam para cobrir quase administra todo-
importante
ção atividades necessárias para gerenciar uma configuração de rede Linux. O número possível de temas que abrangem quase é ilimitada, por isso, naturalmente, tem sido impossível para incluir tudo o que há para dizer sobre todos os assuntos. Tentámos cobrir os mais importantes e comuns. Descobrimos que os novatos a redes Linux, mesmo aqueles com
sem experiência prévia a sistemas operacionais Unix-like, têm encontrado este livro bom o suficiente para ajudá-los com êxito

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

obter suas configurações de rede do Linux instalado e funcionando e prepará-los para aprender mais.

Há muitos livros e outras fontes de informação a partir do qual você pode aprender qualquer um dos tópicos abordados
este livro (com a possível exceção de algumas das características verdadeiramente Linux específicas, como o fogo Linux-novo
interface parede, o que não é bem documentado em outro lugar) com maior profundidade. Nós fornecemos uma bibliografia para
você
para usar quando você está pronto para explorar mais.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Fontes de Informação

Se você é novo no mundo Linux, há uma série de recursos para explorar e se familiarizar com. Hav-
A garantia do acesso à Internet é útil, mas não essencial.

Linux Documentation Project guias

O Linux Documentation Project é um grupo de voluntários que trabalharam para produzir livros (guias), documentos de HOWTO, e páginas de manual sobre temas que vão desde a instalação até a programação do kernel. O PDL trabalhos incluem:

Linux Installation and Getting Started

Por Matt galês, et al. Este livro descreve como obter, instalar e usar o Linux. Ele inclui um introdutória tutorial Unix e informações sobre os sistemas de administração, o X Window System, e networking.

Sistema Linux Guia de administradores

Por Lars Wirzenius Oja e Joanna. Este livro é um guia para a administração geral do sistema Linux ção e abrange temas como a criação e configuração de usuários, a realização de backups do sistema, configuração dos principais pacotes de software e instalar e atualizar software.

Linux System Administration Made Easy

Por Steve Frampton. Este livro descreve a administração do dia-a-dia e problemas de manutenção de relevância para os usuários do Linux.

Linux Guia Programadores

Por B. Scott Burkett, Goldt Sven, John D. Harper, Sven van der Meer, Matt e galês. Este livro aborda temas de interesse para as pessoas que desejam desenvolver um software aplicativo para Linux.

O Kernel do Linux

Por Rusling A. David. Este livro fornece uma introdução para o kernel do Linux, como é construídos, e como ele funciona. Faça um tour do seu kernel.

O Linux Kernel Module Programming Guide

Por Ori Pomerantz. Este guia explica como escrever os módulos do kernel Linux.

Mais manuais estão em desenvolvimento. Para obter mais informações sobre o LDP deve consultar o seu Mundial Wide Web server em http://www.linuxdoc.org/ ou um de seus muitos espelhos.

documentos HOWTO

Os HOWTOs Linux estão um vasto conjunto de documentos que detalham diversos aspectos do sistema - como a instalação e configuração do software X Window System, ou como escrever em assembly linguagem de programação em Linux. Estes são, geralmente localizado no *HOWTO* subdiretório do sites FTP listados posteriormente, ou eles estão disponíveis na World Wide Web em um dos muitos Linux Documenção sites espelho do projeto. Veja a bibliografia no final deste livro, ou o arquivo *HOWTO-INDEX* para uma lista do que está disponível.

Você pode querer obter o *Howto de Instalação*, Que descreve como instalar o Linux em seu sistema, temperatura, a *Hardware Compatibility HOWTO*, Que contém uma lista de hardware conhecido por trabalhar com Linux, e os *Distribuição HOWTO*, O que listas de fornecedores de software Linux venda em disquete e CD-ROM.

A bibliografia deste livro inclui referências aos documentos HOWTO que estão relacionados com Linux rede.

Linux Perguntas Mais Frequentes

A *Linux Perguntas freqüentes com respostas* (FAQ) contém uma grande variedade de perguntas e respostas sobre o sistema. É uma leitura obrigatória para todos os recém-chegados.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Documentação disponível via FTP

Se você tem acesso ao FTP anônimo, você pode obter toda a documentação Linux acima de vários sites, incluindo metalab.unc.edu: / pub / Linux / docs e tsx-11.mit.edu: / pub / linux / docs.

Estes sites são espelhados por uma série de sites ao redor do mundo.

Documentação disponível via WWW

Existem muitos sites baseados em Linux WWW disponíveis. O local de repouso para o Projeto de Documentação Linux pode ser acessado em http://www.linuxdoc.org/.

O Open Source Writers Guild (OSWG) é um projeto que tem um alcance que vai além do Linux. O OSWG, como este livro, tem o compromisso de defender e promover a sua produção de documentação OpenSource. A OSWG site está em casa http://www.oswg.org:8080/oswg.

Ambos os sites contêm hipertexto (e outros) versões de vários documentos relacionados a Linux.

Documentação disponível comercialmente

Um número de editoras e fornecedores de software publicar as obras do Projeto de Documentação Linux. Dois vendedores são:

Consultores especializados Systems, Inc. (SSC)
http://www.ssc.com/
Edifício dos correios Box 55549 Seattle, WA 98155-0549
1-206-782-7733
1-206-782-7191 (FAX)
sales@ssc.com

e:

Sistemas Linux Labs
http://www.lsl.com/
18300 Drive Tara
Clinton Township, MI 48036
1-810-987-8807
1-810-987-3562 (FAX)
sales@lsl.com

Ambas as empresas vendem compêndios de documentos HOWTO do Linux e da documentação de Linux em formato impresso e forma ligada.

O'Reilly & Associates publica uma série de livros de Linux. Este é um trabalho do Projeto de Documentação Linux, mas a maioria foram criados de forma independente. A sua gama inclui:

Rodando Linux

Um guia de instalação e de usuário para o sistema que descreve como obter o máximo de dados pessoais computação com o Linux.

Aprender Debian GNU / Linux
Aprendendo Red Hat Linux

Mais fundamental do que *Rodando Linux*, Esses livros contêm distribuições populares em CD-ROM e de- fer direções robusto para configurá-los e usá-los.

Linux in a Nutshell

Outro na bem-sucedida ", em poucas palavras" série, este livro se concentra em fornecer um amplo referem- texto de referência para Linux.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Linux Jornal e Revista Linux

Linux Journal e *Linux Magazine* são revistas mensais para a comunidade Linux, escrito e publicado por uma número de ativistas Linux. Eles contêm artigos que vão desde perguntas e respostas para novatos programa kernel ming internos. Mesmo se você tiver acesso à Usenet, as revistas são uma boa maneira de ficar em contato com o Linux da comunidade.

Linux Journal é a mais antiga revista e é publicado pela S.S.C. Incorporated, para o qual foram listados os detalhes pré-riormente. Você também pode encontrar a revista sobre a World Wide Web em http://www.linuxjournal.com/.

Linux Magazine é uma nova publicação independente. O site da casa para a revista é http://www.linuxmagazine.com/.

Usenet Newsgroups Linux

Se você tem acesso a notícias Usenet, os seguintes grupos de notícias relacionados ao Linux estão disponíveis:

comp.os.linux.announce

: Um grupo moderado que contenham anúncios de novos softwares, distribuições, relatórios de bugs, e go-Ings-on na comunidade Linux. Todos os usuários do Linux deve ler-se a este grupo. As inscrições podem ser enviadas para linux-announce@news.ornl.gov.

comp.os.linux.help

: Perguntas e respostas gerais sobre como instalar ou usar o Linux.

comp.os.linux.admin

: As discussões relativas à administração de sistemas em Linux.

comp.os.linux.networking

: As discussões relativas à criação de redes com Linux.

comp.os.linux.development

: As discussões sobre o desenvolvimento do kernel do Linux eo sistema em si.

comp.os.linux.misc

: A pega-tudo newsgroup para discussões diversas que não se enquadram nas categorias anteriores.

Há também vários grupos de notícias dedicado ao Linux em outros idiomas além do Inglês, como em fr.comp.os.linux Francês e em alemão de.comp.os.linux.

Listas de discussão Linux

Há um grande número de listas de discussão especializados em Linux que você vai encontrar muitas pessoas dispostas a ajudar com
dúvidas que possa ter.

A mais conhecida delas é a lista organizada pela Rutgers University. Você pode assinar as listas enviando uma mensagem de email formatado como segue:

```
Para: majordomo@vger.rutgers.edu
Assunto: nada
Corpo:
```

Inscrever-se *listname*

Algumas das listas disponíveis relacionados com a rede do Linux são:

linux-net

: Discussões relacionadas a criação de redes Linux

linux-ppp

: Discussões relacionadas com a execução do PPP Linux

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

linux-kernel

Discussões relacionadas ao desenvolvimento do kernel Linux

Suporte Online Linux

Há muitas maneiras de obter ajuda on-line, onde os voluntários de todo o mundo oferecem conhecimentos e serviços, vícios para auxiliar os usuários com dúvidas e problemas.

O EFNET IRC Network é uma rede de IRC dedicado inteiramente ao Open Projects - Open Source e Open Hardware iguais. Alguns de seus canais são projetados para fornecer serviços de suporte online Linux. IRC significa Internet Relay Chat, e é um serviço de rede que lhe permite falar de forma interativa na internet para outros usuários. redes de IRC suporte de múltiplos canais nos quais grupos de pessoas falam. Tudo o que digitar em um canal é visto por todos os outros usuários desse canal.

Há um número de canais ativos na rede de IRC EFNET onde você vai encontrar usuários 24 horas por dia, 7 dias por semana que estão dispostos e aptos a ajudá-lo a resolver os problemas do Linux você pode ter, ou apenas conversar.
Você pode usar este serviço, instalando um cliente de IRC como *irc-II*, Ligando para servername *irc.openprojects.org: 6667*, E juntando o `# Linpeople` canal.

Grupos de usuários Linux

Muitos grupos de usuários Linux ao redor do mundo oferecem suporte direto aos usuários. Muitos grupos de usuários Linux se envolver em atividades como dias de instalação, palestras e seminários, noites de demonstração, e outros eventos sociais completamente. Grupos de Usuários Linux são uma ótima maneira de encontrar outros usuários do Linux em sua área. Há uma série de publicações listas de grupos de usuários Linux. Algumas das marcas mais conhecidas são:

Grupos de Usuários Linux Everywhere

http://www.ssc.com/glue/groups/

LUG projeto lista

http://www.nllgg.nl/lugww/

Registro LUG

http://www.linux.org/users/

Obter Linux

Não há distribuição individual do software Linux, em vez disso, existem muitas distribuições, como Debian, RedHat, Caldera, SuSE Corel, e Slackware. Cada distribuição contém tudo que você precisa para executar um completo Sistema Linux: o kernel, utilitários básicos, bibliotecas, arquivos, suporte e aplicações de software.

distribuições Linux podem ser obtidas através de várias fontes online, como a Internet. Cada uma das principais distribuições tem seu próprio FTP e web site. Alguns destes sites são:

Caldera

http://www.caldera.com/ftp://ftp.caldera.com/

Corel

http://www.corel.com/ftp://ftp.corel.com/

Debian

http://www.debian.org/ftp://ftp.debian.org/

RedHat

http://www.redhat.com/ftp://ftp.redhat.com/

Slackware

http://www.slackware.com/ftp://ftp.slackware.com/

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

SuSE

http://www.suse.com/ftp://ftp.suse.com/

Muitos dos sites populares de arquivo geral FTP também espelho de várias distribuições Linux. O mais conhecido destes sites são:

metalab.unc.edu: / pub / Linux / distribuições
ftp.funet.fi: / pub / Linux / mirrors /
TSX 11.mit.edu: / pub / linux / distribuições
mirror.aarnet.edu.au: / pub / linux / distribuições

Muitas das distribuições modernas podem ser instalados diretamente da Internet. Há um monte de software para download para uma instalação típica, porém, assim que você provavelmente quer fazer isso somente se você tiver uma alta velocidade,
ligação permanente à rede, ou se você só precisa atualizar uma instalação existente.[1]

Linux pode ser adquirido em CD-ROM a partir de um número crescente de fornecedores de software. Se o seu computador local loja não tem isso, talvez você deve pedir-lhes para estocá-lo! A maioria das distribuições mais populares podem ser obtidas em CD-ROM. Alguns fornecedores de produtos com múltiplos CD-ROMs, cada um dos quais fornece uma dife-distribuição Linux ent. Esta é uma maneira ideal para experimentar uma série de distribuições diferentes antes de se decidir sobre o seu
um favorito.

Arquivo de Normas do Sistema

No passado, um dos problemas que afligiam as distribuições Linux, assim como os pacotes de software em execução Linux, foi a falta de um esquema único sistema de arquivos aceitos. Isto resultou em discordâncias entre os diferentes pacotes, e os usuários e administradores de confrontado com a tarefa de localizar vários arquivos e programas.

Para melhorar esta situação, em agosto de 1993, várias pessoas formaram o Linux File System Standard Group (FSSTND). Após seis meses de discussão, o grupo criou um projecto que apresenta uma estrutura coerente de arquivo sytem e define a localização dos programas mais essenciais e arquivos de configuração.

Esta norma deveria ter sido aplicado pela maioria das distribuições de Linux e pacotes. É um
pouco lamentável que, enquanto a maioria das distribuições ter feito alguma tentativa de trabalhar para a FSSTND, há uma número muito pequeno de distribuições, que foi realmente aprovado na íntegra. Ao longo deste livro, vamos supor que quaisquer arquivos discutido residem no local especificado pela norma; localizações alternativas serão mencionados apenas quando há uma longa tradição que os conflitos com esta especificação.

O FSSTND Linux continuou a desenvolver, mas foi substituído pelo arquivo Linux Hierarchy Standard (FHS), em 1997. A ESF aborda as questões de arquitetura multi que o FSSTND não. O FHS podem ser obtidas
diretório de documentação do Linux de todos os principais sites FTP Linux e seus espelhos, ou no seu home-site http://www.pathname.com/fhs/.Daniel Quinlan, o coordenador do grupo de ESF, pode ser alcançado em quinlan@transmeta.com.

Linux Standard Base

O grande número de diferentes distribuições Linux, oferecendo muitas opções de escolha saudável para os usuários do Linux,

tem
criou um problema para desenvolvedores de software - principalmente os desenvolvedores de software não-livre.

Cada pacotes de distribuição e suprimentos bibliotecas certa base, ferramentas de configuração, aplicações do sistema, e con-arquivos de configuração. Infelizmente, as diferenças em suas versões, nomes e locais tornam muito difícil saber
o que existe em qualquer distribuição. Isso torna difícil para desenvolver aplicativos binários que funcionará confiavelmente em todas as bases de distribuição Linux.

Para ajudar a superar esse problema, um novo projeto surgiu o chamado "Linux Standard Base". Destina-se a descrever uma distribuição de base padrão que as distribuições cumprimento usará. Se um desenvolvedor projeta um aplicativo para trabalhar

1 ... ou você é muito impaciente e sei que as 24 horas que pode demorar para baixar o software a partir da Internet é mais rápido do que o 72 horas, pode levar a esperar por um CD-ROM a ser entregue!

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

contra a plataforma de base padrão, o aplicativo vai funcionar, e ser portátil, a qualquer distribuição Linux cumprindo-
ção.

Você pode encontrar informações sobre o status do projeto Linux Standard Base, na sua casa no site
http://www.linuxbase.org/.

Se você estiver preocupado com a interoperabilidade, nomeadamente de software de fornecedores comerciais, você deve

assegurar
que a sua distribuição Linux está fazendo um esforço para participar do projeto de normalização.

Sobre este livro

Quando Olaf se juntou ao Projeto de Documentação Linux em 1992, ele escreveu dois capítulos sobre o UUCP e pequenas

`smail`,
que pretende contribuir para o Guia do Administrador do Sistema. Desenvolvimento de redes TCP / IP estava apenas
início e, quando os "capítulos pequenos" começaram a crescer, ele perguntou em voz alta se seria bom ter
um Guia de Rede. "Ótimo!" todos diziam. "Go for it!" Então ele foi para ela e escreveu a primeira versão do
Networking Guide, que foi lançado em setembro de 1993.

Olaf continuou a trabalhar sobre o Guia de Rede e finalmente produziu uma versão muito melhorada do guia.
Vince Skahan contribuiu com o original `sendmail` capítulo mail, que foi completamente substituído nesta edição
por causa de uma nova interface para o `sendmail` configuração.

A versão do guia que você está lendo agora é uma revisão e atualização solicitado pela O'Reilly & Associates
e realizado por Terry Dawson.[2] Terry foi um operador de rádio amador para mais de 20 anos e já trabalhou em
o setor de telecomunicações há mais de 15 deles. Ele foi co-autor do original NET-FAQ, e desde então tem
de autoria e mantido vários documentos HOWTO relacionada com rede. Terry sempre foi um entusiasta
apoiante do projecto da Rede Guia de administradores, e acrescentou alguns capítulos novos para esta versão descrevendo
características de rede do Linux que têm sido desenvolvidos desde a primeira edição, mais um monte de mudanças para trazer
o resto do livro até à data.

A `exim` capítulo foi contribuído por Philip Hazel[3] que é um dos principais desenvolvedores e mantenedores do pacote.

O livro está organizado aproximadamente ao longo da seqüência de passos que você deve tomar para configurar seu sistema para

a rede-
de trabalho. Ele começa por discutir os conceitos básicos de redes e redes TCP / IP baseados em particular. Em seguida,
trabalhar lentamente é uma maneira acima de configurar o TCP / IP no nível do dispositivo de firewall, contabilidade e
mascarada
configuração, para a instalação de aplicativos comuns, como `rlogin` e amigos, o Network File System, e
o Sistema de Informação de Rede. Isso é seguido por um capítulo sobre como configurar sua máquina como um nó de UUCP.
A maioria das seções restante é dedicado a duas principais aplicações que rodam no topo do TCP / IP e UUCP:
correio eletrônico e notícias. Um capítulo especial foi dedicado ao protocolo IPX eo sistema de arquivos NCP, ser-
porque estas são usadas em muitos ambientes corporativos, onde o Linux é encontrar um lar.

A parte de e-mail apresenta uma introdução às partes mais íntimas de transporte de correio e encaminhamento, e da miríade
de esquemas de endereçamento você pode ser confrontado. Ele descreve a configuração e gestão de `exim`, Um
agente de transporte de correio ideal para uso na maioria das situações que não requerem UUCP, e `sendmail`, Que é para as
pessoas
que têm de fazer mais complicadas de roteamento envolvendo UUCP.

A parte da notícia dá uma visão geral de como funciona notícias Usenet. Abrange INN e C News, os dois mais
amplamente utilizados pacotes de notícias software de transporte, no momento, eo uso de NNTP para fornecer newsreading
acesso a uma rede local. O livro termina com um capítulo sobre o cuidado ea alimentação dos mais populares NewsLer-
ers em Linux.

É claro que um livro nunca pode exaustivamente responder todas as perguntas que você possa ter. Então, se você seguir as

instruções
neste livro, e algo que ainda não funciona, por favor, seja paciente. Alguns de seus problemas pode ser devido a erros
da nossa parte (veja a seção ", posteriormente neste Prefácio), mas eles também podem ser causadas por mudanças na rede
software. Portanto, você deve verificar os recursos de informação listadas primeiro. Há uma boa chance de que você está
não está sozinho com seus problemas, então fixar um ou pelo menos uma solução alternativa proposta é susceptível de ser

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

conhecido. Se você tiver a
oportunidade, você também deve tentar obter a última versão do kernel e de rede de um dos sites FTP Linux ou um BBS perto de você. Muitos problemas são causados por software de diferentes estágios de desenvolvimento, que não trabalham junto corretamente. Afinal, o Linux é um "work in progress".

2 Terry Dawson pode ser alcançado em terry@linux.org.au
3 Philip Hazel pode ser alcançado em ph10@cus.cam.ac.uk

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O Oficial Versão Impressa

No Outono de 1993, Andy Oram, que tinha sido em torno da lista de discussão LDP de quase desde o começo, pediu Olaf sobre a publicação deste livro na O'Reilly & Associates. Ele estava animado com esse livro, nunca ter ima- INED que se tornaria este sucesso. Ele e Andy finalmente acordado que O'Reilly produziria um reforço Versão Impressa Oficial do Guia de Rede, enquanto Olaf manteve o autor original, de modo que a fonte do livro pode ser distribuído gratuitamente. Isso significa que você pode escolher livremente: você pode obter as várias formas livres do documento de seu mais próximo do Linux Documentation Project site espelho e imprimi-lo, ou você pode comprar o funcionário versão impressa da O'Reilly.

Por que, então, que você iria querer pagar por algo que você pode obter de graça? Tim O'Reilly é fora de sua mente para a publicação de algo que todo mundo pode imprimir e até mesmo vender-se?[4] Existe alguma diferença entre esses versões?

As respostas são: "depende", "Não, definitivamente não", e "sim e não." O'Reilly & Associates é preciso ser um risco em publicar o Guia de Rede, e parece ter dado certo para eles (eles nos pediram para fazê-lo novamente). Nós acredito que este projeto serve como um excelente exemplo de como o mundo do software livre e as empresas podem cooperar para produzir algo que ambos podem se beneficiar. Em nossa opinião, o grande serviço de O'Reilly é proporcionar aos com Linux Comunidade (para além do livro tornar-se facilmente disponível na sua livraria local) é que ele ajudou a ser-Linux se reconhecido como algo a ser levado a sério: uma alternativa viável e útil para operat comerciais outras mento dos sistemas. É uma livraria triste técnico que não tenha pelo menos uma prateleira com livros empilhados O'Reilly Linux.

Por que eles são de publicá-lo? Eles vêem isso como seu tipo de livro. É o que eles esperam produzir, se contratada com um autor a escrever sobre o Linux. O ritmo, o nível de detalhe, e se encaixam no estilo de bem com suas outras ofertas.

A questão da licença LDP é ter a certeza que ninguém fica fechada para fora. Outras pessoas podem imprimir cópias deste livro, e ninguém vai culpar você, se você pegar um desses exemplares. Mas se você não tiver começado a chance de ver o O'Reilly versão, tentar chegar a uma livraria ou olhar para copiar de um amigo. Nós pensamos que você gosta do que vê, e vai querer comprá-lo por si mesmo.

Assim que sobre as diferenças entre as versões impressa e on-line? Andy Oram tem feito grandes esforços na transformando o nosso divagações em algo realmente vale a pena imprimir. (Ele também analisou alguns outros livros produzido pelo Projeto de Documentação Linux, o que contribui de qualificação profissional que pode para o Linux comunidade).

Desde que Andy começou a revisar o Guia de Rede e edição de cópias enviadas a ele, o livro tem melhorado muito da sua forma original, e com cada rodada de apresentação e comentários melhora novamente. A oportu- oportunidade para tirar vantagem da habilidade de um editor profissional é um não deve ser desperdiçada. Em muitos aspectos, a contribuição de Andy foi tão importante quanto o dos autores. O mesmo vale também para a editores de texto, que tem o livro no forma você vê agora. Todas estas edições têm sido alimentado de volta para a versão online, então não há diferença na con- barraca.

Ainda assim, a versão O'Reilly *vai* ser diferente. Será profissionalmente ligado, e quando você pode ir para o trabalho para imprimir a versão gratuita, é pouco provável que você irá obter o resultado a mesma qualidade, e mesmo assim, é mais improvável que você vai fazer isso para o preço. Em segundo lugar, as nossas tentativas amadora de ilustração terá sido substituído por bem refeito figuras por artistas profissionais da O'Reilly. Indexadores têm gerado um índice melhorou, o que faz localização de informações no livro um processo muito mais simples. Se este livro é algo que você pretende ler do início para finalizar, você deve considerar a leitura da versão oficial impresso.

Resumo

Capítulo 1, *Introdução às Redes*, Discute a história do Linux e abrange as informações básicas de rede no UUCP, TCP / IP, vários protocolos, hardware e segurança. Os próximos capítulos tratam poucos com a configuração do Linux para a rede TCP / IP e execução de algumas aplicações importantes. Examinamos IP de um pouco mais de perto no capítulo 2, *Problemas de rede TCP / IP*, Antes de começar nossas mãos sujas com a edição de arquivos e assim por diante. Se você já sabe como funciona e roteamento IP e como a resolução de endereço é realizada, você pode pular este capítulo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

4 Note que enquanto você está autorizado a imprimir a versão on-line, você pode *não* executar o livro da O'Reilly através de uma copiadora, e muito menos vender
qualquer um dos seus (hipotético) cópias

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 3, *Configurando o hardware de rede*, Lida com problemas de configuração bem básica, tais como a construção de uma kernel e configurar sua placa Ethernet. A configuração de suas portas seriais é coberto separadamente no Capítulo 4 º, *Configurando o Hardware Serial*, Porque a discussão não se aplica a redes TCP / IP apenas, mas é também relevante para o UUCP.

Capítulo 5, *Configurando Redes TCP / IP*, Ajuda a configurar sua máquina para a rede TCP / IP. Ele contém dicas de instalação para os anfitriões autônomo com loopback habilitada apenas, e os hosts conectados a uma rede Ethernet. Ele também apresenta-lhe algumas ferramentas úteis que você pode usar para testar e depurar sua configuração. Capítulo 6, *Nome do serviço e Resolver Configuração*, Explica como configurar resolução de nomes e explica como configurar um servidor de nome.

Capítulo 7, *Serial Line IP*, Explica como estabelecer conexões SLIP e dá uma referência pormenorizada de `mergulho`, Um ferramenta que permite automatizar a maioria das medidas necessárias. Capítulo 8, *O protocolo ponto-a-Ponto*, Abrange PPP e `pppd`, O daemon PPP.

Capítulo 9, *Firewall TCP / IP*, Estende-se a nossa discussão sobre a segurança da rede e descreve o protocolo TCP / Linux, firewall IP e suas ferramentas de configuração: `ipfwadm`,`ipchains`E `iptables`. firewall IP fornece um meio de controle ling quem pode acessar sua rede e hosts com muita precisão.

Capítulo 10, *IP Contabilidade*, Explica como configurar o IP de Contabilidade no Linux para que você possa acompanhar como muito tráfego está indo para onde e que está gerando isso.

Capítulo 11, *IP Masquerade e Network Address Translation*, Abrange uma característica da rede Linux software mascarado chamado IP, que permite que todas as redes IP para se conectar e utilizar a Internet através de um único Endereço IP, escondendo os sistemas internos de fora no processo.

Capítulo 12, *Rede Características importantes*, Dá uma breve introdução à criação de alguns dos mais importantes aplicações de rede, tais como `rlogin`,`ssh`, Etc Este capítulo também aborda como os serviços são geridos pelo `inetd` superusuário, e como você pode restringir determinados serviços relevantes para a segurança de um conjunto de hosts confiáveis.

Capítulo 13, *O Sistema de Informação de Rede*E capítulo 14, *O Network File System*, Discutir NIS e NFS. NIS é uma ferramenta usada para distribuir informações administative, tais como senhas de usuários em uma rede de área local. NFS permite compartilhar entre sistemas de arquivos de diversas máquinas em sua rede.

No capítulo 15, *IPX eo sistema de arquivos NCP*, Discutimos o protocolo IPX eo sistema de arquivos NCP. Estes permitem Linux para ser integrado em um ambiente Novell NetWare, compartilhar arquivos e impressoras com máquinas não-Linux.

Capítulo 16, *Gerenciando UUCP Taylor*, Dá-lhe uma ampla introdução à administração de Taylor UUCP, uma implementação livre do conjunto de UUCP.

O restante do livro é absorvido por um tour detalhado de correio electrónico e de notícias da Usenet. Capítulo 17, *Elec-Por correio electrónico*, Apresenta os conceitos centrais de correio eletrônico, como o que um endereço de e-mail parece, e como o sistema de tratamento de correio consegue chegar a sua mensagem ao destinatário.

Capítulo 18, *Sendmail*E Capítulo 19, *Obter Exim Funcionando*, Cobrir a configuração do `sendmail` e `exim`, Dois agentes de transporte de correio que você pode usar para o Linux. Este livro explica os dois, porque `exim` é mais fácil de instalar para o novato, enquanto `sendmail` fornece suporte para o UUCP.

Capítulo 20, *Netnews*, Através do Capítulo 23, *Internet News*, Explicar a forma como é gerida de notícias na Usenet e como você instalar e usar C News, `nntpd`E DCI: três pacotes de software para gerenciamento de notícias Usenet. Após a breve introdução do capítulo 20, você pode ler o Capítulo 21, *C News*Se você deseja transferir notícias usando C News, um serviço tradicional, geralmente usado com o UUCP. Os capítulos seguintes abordam mais moderno alternativos para C notícias que usam a Internet baseada em protocolo NNTP (Network News Transfer Protocol). Capítulo 22, *NNTP eo Daemon nntpd* explica como configurar um servidor NNTP simples, `nntpd`, Para fornecer a leitura de notícias acesso para uma rede local, enquanto que o Capítulo 23 descreve um servidor mais robusto para NetNews mais ampla transferências, a internet daemon News (DCI). E, finalmente, o Capítulo 24, *Newsreader Configuração*, Mostra-lhe como configurar e manter diversos leitores de notícias.

Convenções usadas neste livro

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Todos os exemplos apresentados neste livro assumem que você está usando um `sh` shell compatível. A `bater` reservatório é `sh` compa-
vel e é o shell padrão de todas as distribuições Linux. Se acontecer de você ser um `csh` usuário, você terá que fazer ajustamentos adequados.

A seguir está uma lista das convenções tipográficas utilizadas neste livro:

Itálico

Usado para arquivos e diretórios, nomes de programa e de comando, opções de linha de comando, endereços de e-mail e caminhos, URLs, e para enfatizar novos termos.

Negrito

Usado para nomes de máquinas, nomes de máquinas, nomes de sites, nomes de usuários e IDs, e para dar ênfase ocasionais.

`Largura Constante`

Usado em exemplos para mostrar o conteúdo de arquivos de código ou a saída de comandos e para indicar ambiente variáveis e palavras-chave que aparecem no código.

Largura Constante Itálico

Usado para indicar opções variáveis, palavras-chave ou texto que o usuário é substituir por um valor real.

Largura Constante em Negrito

Usado em exemplos para mostrar comandos ou outro texto que deve ser digitado literalmente pelo usuário.

AVISO: O texto apresentado dessa maneira oferece um aviso. Você pode cometer um erro aqui que fere seu sis-
temperatura ou é difícil de recuperar.

Enviando alterações

Temos testado e verificou as informações contidas neste livro o melhor de nossa capacidade, mas você pode descobrir que

recursos
mudaram (ou mesmo que cometemos erros!). Por favor informe-nos sobre os erros que você encontrar, bem como suas sugestões para edições futuras, por escrito para:

O'Reilly & Associates, Inc.
101 Morris Street
Sebastopol, CA 95472
1-800-998-9938 (nos os EUA ou Canadá)
1-707-829-0515 (internacional ou local)
1-707-829-0104 (FAX)

Você pode enviar mensagens eletronicamente. Para ser colocado na lista de discussão ou solicitar um catálogo, envie um email

para:

info@oreilly.com

Para esclarecer dúvidas técnicas ou comentários sobre o livro, envie um email para:

bookquestions@oreilly.com

Temos um site para o livro, onde nós vamos listar exemplos, errata e quaisquer planos para futuras edições. Você pode acessar essa página em:

http://www.oreilly.com/catalog/linag2

Para obter mais informações sobre este livro e outros, consulte o site da O'Reilly:

http://www.oreilly.com/

Agradecimentos

Esta edição do Guia de Rede deve quase tudo ao excelente trabalho de Olavo e Vince. É
difícil de apreciar o esforço que vai para pesquisar e escrever um livro desta natureza até que você tenha um

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

chance de trabalhar em um você mesmo. Atualizando o livro foi uma tarefa desafiadora, mas com uma excelente base para o trabalho
da, foi muito agradável.

Este livro deve muito às numerosas pessoas que aproveitou o tempo para a prova a lê-lo e ajudar a resolver muitos erros, tanto técnica e gramatical (nunca soube que existia uma coisa como um particípio dangling). Phil Hughes, John Macdonald, e Erik Ratcliffe todos desde muito útil (e em geral, bastante consistente) feed-volta sobre o conteúdo do livro.

Também devo muito obrigado ao povo da O'Reilly que tivemos o prazer de trabalhar com: Sarah Jane Shangraw, que tenho o livro na forma que você pode ver agora, Maureen Dempsey, que editada do texto; Rob Romano, Rhon Porter, e Chris Reilley, que criou todas as figuras; Hanna Dyer, que desenhou a capa; Alicia Cech, Futato David e Jennifer Niedherst para o layout interno; Lars Kaufman para sugerir xilogravuras de idade como um tema visual; Judy Hoer para o índice e, finalmente, Tim O'Reilly para a coragem de assumir um projeto como este.

Temos uma grande dívida para Andres Sepúlveda, Wolfgang Michaelis, K. Michael Johnson, e todos os desenvolvedores que poupado o tempo para verificar as informações prestadas na Guia de Rede. Phil Hughes, John MacDonald, e Eric Ratcliffe contribuiu com observações inestimáveis sobre a segunda edição. Gostaríamos também de agradecer a todos aqueles que lêem
a primeira versão do Guia de Rede e as correções e sugestões enviadas. Você pode encontrar uma com sorte-uma lista completa de colaboradores no arquivo *Graças* na distribuição online. Finalmente, este livro não teria sido possível sem o apoio do Holger Grothe, que forneceu Olaf com a conectividade com a Internet que ele precisava fazer a versão original acontecer.

Olaf também gostaria de agradecer aos seguintes grupos e empresas que imprimiu a primeira edição do Networking Guia e doaram dinheiro, seja para ele ou para o Projeto de Documentação Linux como um todo: Suporte Linux Team, Erlangen, Alemanha; S.u.S.E. GmbH, Fürth, Alemanha;. Labs e Linux System, Inc., Twp Clinton, Estados Unidos, Software RedHat, North Carolina, Estados Unidos.

Terry graças a sua mulher, Maggie, que pacientemente suportado por toda a sua participação no projeto, apesar os desafios apresentados pelo nascimento de seu primeiro filho, Jack. Além disso, ele agradece a *muitos* pessoas do Linux comunidade que tanto alimentou ou sofrido até o ponto em que ele realmente pode participar e ac-vamente contribuir. "Eu vou te ajudar se você prometer ajudar alguém em troca."

O Hall da Fama

Além daqueles já mencionados, um grande número de pessoas que tenham contribuído para o Guia de Rede, analisando-a e enviando correções e sugestões. Estamos muito gratos.

Aqui está uma lista daqueles cujas contribuições deixaram um rastro em pastas nosso e-mail.

Al Longyear, Alan Cox, Andres Sepúlveda, Ben Cooper, Spitzer Cameron, Colin McCormack, DJ Roberts, Lopes Emilio, Fred N. van Kempen, Gert Doering, Greg Hankins, Eissfeldt Heiko, Szikora JP, Johannes Stille, Karl Eichwalder, Les Johnson, Ludger Kunz, Marc van Diest, Michael K. Johnson, Nebel Michael, Michael Asa de Mitch, D'Souza, Gortmaker Paulo, Brouwer Peter, Peter Eriksson, Phil Hughes, Miller Deluth Raul, Rich Braun, Sladkey Rick, Aarts Ronald, Thüemmler Swen, Terry Dawson, Thomas Quinot, e Shevchuk Yury.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 1 - Introdução às Redes

História

A idéia da rede é provavelmente tão antigo quanto as telecomunicações em si. Considere as pessoas que vivem na Idade da

Pedra,
quando a bateria pode ter sido usada para transmitir mensagens entre os indivíduos. Suponha que um homem das cavernas quer convidar
B caveman para um jogo de atirar pedras um no outro, mas eles vivem muito longe de B para ouvir um barulho dele
tambor. Quais são as opções de A? Podia 1) caminhada até a casa de B, 2) obter um maior tambor, ou 3) pedir C, que vive a meio caminho entre eles, para encaminhar a mensagem. A última opção é chamada *rede*.

É claro que temos um longo caminho desde as perseguições primitiva e dispositivos de nossos antepassados. Hoje em dia, têm computadores conversem entre si sobre vastos conjuntos de fios, fibra óptica, microondas, etc, para fazer um compromisso para a partida de sábado de futebol.[5] Na descrição a seguir, nós vamos lidar com os meios e formas por que isso é feito, mas deixar de fora os fios, bem como a parte do futebol.

Nós iremos descrever três tipos de redes neste guia. Iremos nos concentrar em TCP / IP mais fortemente porque é o conjunto de protocolos mais popular utilizada por ambas as Local Area Networks (LANs) e Wide Area Networks (WANs), como a Internet. Também vamos dar uma olhada no UUCP e IPX. UUCP já foi comumente utilizados para o transporte notícias e mensagens de correio através de ligações de telefone dial-up. É menos comum hoje, mas ainda é útil em uma variciedade de situações. O protocolo IPX é usado mais comumente em ambiente Novell NetWare e nós descreva como usá-lo para conectar a sua máquina Linux em uma rede Novell. Cada um destes protocolos estão em rede ção de protocolos e são usadas para transportar dados entre computadores. Vamos discutir como eles são usados e introduzir que seus princípios subjacentes.

Nós definimos uma rede como uma coleção de *hosts* que são capazes de se comunicar uns com os outros, muitas vezes

apoiando-se em
os serviços de um número de servidores dedicados, que retransmitem os dados entre os participantes. Hosts são frequentemente computadores,
mas não precisa ser, pode-se pensar também em terminais X ou impressoras inteligentes como anfitriões. pequenas aglomerações de hosts
também são chamados *sites*.

A comunicação é impossível sem algum tipo de linguagem ou código. Em redes de computadores, essas linguagens são coletivamente denominados *protocolos*. No entanto, você não deve pensar em protocolos escritos aqui, mas sim da código altamente formalizada de comportamento observado quando os chefes de estado se reúnem, por exemplo. De forma muito semelhante,
os protocolos usados em redes de computadores nada mais são regras muito rígidas para a troca de mensagens entre dois ou mais hosts.

Redes TCP / IP

aplicações de rede modernos exigem uma sofisticada abordagem para transportar dados de uma máquina para outra.
Se você estiver administrando uma máquina Linux, que tem muitos usuários, cada um dos quais pode querer se conectar simultaneamente a
hosts remotos em uma rede, você precisa encontrar uma maneira de deixá-los para compartilhar sua conexão de rede sem interferên-
ção com o outro. A abordagem que um grande número de protocolos de rede moderna usa é chamado *pacotes comutação*. A *pacote* é um pequeno pedaço de dados que são transferidos de uma máquina para outra através da rede.
A mudança ocorre quando o datagrama é realizada em cada elo da rede. A comutação de pacotes de rede
partes uma relação única rede entre diversos usuários pela alternadamente envio de pacotes de um usuário para outro através afluentes.

A solução que os sistemas Unix, e posteriormente muitos sistemas não-Unix, ter adoptado é conhecido como TCP / IP.
Quando se fala em redes TCP / IP que você vai ouvir o termo *datagrama*, Que, tecnicamente, tem um significado especial mas é muitas vezes usado como sinônimo de *pacote*. Nesta seção, vamos dar uma olhada em conceitos de base do Protocolos TCP / IP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

5 O espírito original de que (veja acima) mostra ainda, em algumas ocasiões na Europa

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Introdução às redes TCP / IP

TCP / IP traça suas origens a um projeto de pesquisa financiado pelos Estados Unidos Defense Advanced Research Projects Agency (DARPA), em 1969. A ARPANET era uma rede experimental que foi convertido em uma operação uma em 1975, após ter provado ser um sucesso.

Em 1983, o novo protocolo suite TCP / IP foi adotado como um padrão, e todos os hosts da rede eram obrigados a usá-lo. Quando finalmente ARPANET cresceu na Internet (ARPANET saindo de existência em 1990), o uso do TCP / IP já havia se espalhado para as redes para além da própria Internet. Muitas empresas têm construído agora corporativa
Redes TCP / IP, e da Internet tem crescido a um ponto em que ele quase poderia ser considerado um mainstream tecnologia de consumo. É difícil ler um jornal ou uma revista sem ver agora referência para a Inter-líquido; quase todos agora podem usá-lo.

Para algo concreto para olhar como discutimos TCP / IP em toda as seguintes seções, vamos considerar Groucho Marx University (GMU), situado algures no Fredland, como um exemplo. A maioria dos departamentos executar suas próprias redes de área local, enquanto uma certa ação e outros correm vários deles. Eles estão todos interligados e ligado à Internet através de uma ligação de alta velocidade única.

Suponha que uma máquina Linux é conectado a uma rede local de hosts Unix no departamento de Matemática, e seu nome é *Erdos*. Para acessar um host no Departamento de Física, por exemplo *quark*, Você digite o seguinte comando:

```
$ quark.physics rlogin
Bem-vindo ao Departamento de Física da GMU
(Ttyq2) login:
```

No prompt, você digita seu nome de login, digamos *andres*, E sua senha. Está dado então um shell[6] em *quark*, para o qual você pode digitar como se você estivesse sentado no console do sistema. Depois que você sair da shell, você volta para
sua própria máquina de alerta. Você tem usado apenas um dos instantânea, aplicações interativas que o TCP / IP dispõe: login remoto.

Ao ser conectado ao *quark*, Você também pode querer executar um aplicativo de interface gráfica do usuário, como uma palavra programa de processamento, um programa de desenho gráfico, ou mesmo uma World Wide Web browser. O sistema X Windows
é um ambiente de usuário totalmente ciente de redes gráfica, e está disponível para muitos sistemas de computação. Para contar essa aplicação que você quer ter suas janelas exibidas na tela do seu anfitrião, você tem que definir o *DISPLAY* variável de ambiente:

```
$ erdos.maths DISPLAY =: 0.0
$ export DISPLAY
```

Agora, se você iniciar o aplicativo, ele irá contatar o servidor X em vez de *quark*'S, e mostrar todas as suas janelas em sua tela. Claro, isso requer que você tenha X11 runnning em *Erdos*. O ponto aqui é que o TCP / IP permite que *quark* e *Erdos* para enviar pacotes X11 para trás e para dar-lhe a ilusão de que você está em um único sistema. A rede é quase transparente aqui.

Outra aplicação muito importante em redes TCP / IP é o NFS, o que representa *Network File System*. É outra forma de tornar a rede transparente, porque basicamente permite que você trate hierarquias de diretórios de outras máquinas como se fossem sistemas de arquivos locais e parecido com outros diretórios no seu host. Por exemplo, todos os diretórios home dos usuários podem ser mantidos em uma máquina servidor central do qual todos os outros hosts na rede local de montagem
elas. O efeito é que os usuários podem efetuar login em qualquer máquina e se encontram no diretório home do mesmo. Simi-particularmente, é possível compartilhar grandes quantidades de dados (como um banco de dados, documentação ou programas de aplicação)
entre vários hosts através da manutenção de uma cópia dos dados em um servidor e permitir que outros hosts para acessá-lo. Nós voltar para NFS no Capítulo 14, *O Network File System*.

Naturalmente, estes são apenas exemplos do que você pode fazer com redes TCP / IP. As possibilidades são quase ilimitado menos, e vamos apresentá-lo a mais como você lê sobre o livro.

Vamos agora ter um olhar mais atento à forma como TCP / IP funciona. Esta informação ajudará a entender como e porque você tem que configurar sua máquina. Vamos começar examinando o hardware e, lentamente, o nosso modo de trabalho para cima.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

6 O shell é uma interface de linha de comando para o sistema operacional Unix. É semelhante ao prompt do DOS em um ambiente Windows da Microsoft mento, embora muito mais poderoso

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Ethernets

O tipo mais comum em hardware LAN é conhecido como *Ethernet*. Em sua forma mais simples, consiste em um único cabo com hosts conectados a ele através de conectores, torneiras, ou emissores-receptores. Ethernets simples são relativamente baratos
instalação, que juntamente com uma taxa de transferência líquida de 10, 100 ou até 1.000 Megabits por segundo, responsável por grande parte
de sua popularidade.

Ethernets vêm em três sabores: *espessura,fina*E *de par trançado*. Ethernet fino e grosso de cada utilização de um cabo coaxial, diferentes em diâmetro e da maneira que você pode anexar um host para esse cabo. Thin Ethernet usa uma forma de T "BNC" conector, que é inserido o cabo e torcer para um plugue na parte traseira do computador. Thick Ethernet
requer que você faça um pequeno orifício no cabo, e anexar um transceptor usando um "vampiro da torneira." Um ou mais hosts podem então ser ligado ao transmissor. cabo Ethernet finos e grossos pode ser executado por um período máximo de 200 e 500 metros, respectivamente, e são também chamados 10BASE-2 e 10Base-5. A "base" refere-se a "banda de modulação" e simplesmente significa que os dados é alimentado diretamente no cabo sem modem. O número refere-se no início à velocidade em Megabits por segundo, eo número no final é o comprimento máximo do cabo em centenas
de metros. de par trançado utiliza um cabo feito de dois pares de fios de cobre e geralmente requer hardware adicional conhecido como *hubs ativos*. de par trançado é também conhecido como 10Base-T, o "T", significando par trançado. Os 100 Megabits
por segunda versão é conhecida como 100BASE-T.

Para adicionar um host para uma instalação Ethernet fino, tem que interromper o serviço de rede por pelo menos alguns minutos, ser-
Porque você tem que cortar o cabo para inserir o conector. Embora a adição de um host a um sistema Ethernet grosso é um pouco complicado, normalmente não derrubar a rede. Ethernet de par trançado é ainda mais simples. Ele usa um dispositivo chamado "hub", que serve como um ponto de interligação. Você pode inserir e retirar os hosts de um hub sem interromper os usuários em todos os outros.

Muitas pessoas preferem fino Ethernet para redes pequenas, pois é muito barato; PC Cards vêm por tão pouco como EUA $ 30 (muitas empresas estão, literalmente, jogá-las fora agora), eo cabo está na faixa de alguns centavos por metros. No entanto, para as instalações de grande escala, seja grosso ou Ethernet de par trançado é mais adequado. Por exemplo, a Ethernet em Matemática GMU Departamento originalmente escolheu Ethernet grosso, porque é um longo caminho que o cabo deve tomar para o tráfego não será interrompido cada vez que um host for adicionado à rede. de par trançado instalações são muito comuns em uma variedade de instalações. O hardware Hub está caindo de preço e pequena
unidades estão agora disponíveis a um preço que seja atraente até mesmo para pequenas redes domésticas. Par trançado pode ser significativamente mais barato para grandes instalações, eo cabo em si é muito mais flexível do que os cabos coaxiais utilizado nos sistemas de Ethernet outras. Os administradores de rede do departamento de matemática da GMU está planejando para substituir a rede existente, com uma rede de par trançado no ano que vem finanical porque trará
los atualizados com a tecnologia atual e salvá-los de tempo significativo, quando a instalação de computadores novos hospedeiros
e movendo-se em torno de computadores existentes.

Uma das desvantagens da tecnologia Ethernet é o seu comprimento de cabo limitada, o que impede qualquer utilização do mesmo que não seja
para redes locais. No entanto, vários segmentos Ethernet pode ser ligado a um outro usando repetidores, bridges ou roteadores. Os repetidores simplesmente copiar os sinais entre dois ou mais segmentos para que todos os segmentos juntos agem como se é um Ethernet. Devido às exigências do calendário, não pode haver mais de quatro repetidores entre quaisquer dois hosts na rede. Pontes e roteadores são mais sofisticados. Eles analisam os dados recebidos e encaminhá-lo apenas quando o host receptor não está no local Ethernet.

Ethernet funciona como um sistema de ônibus, onde um host pode enviar pacotes (ou *quadros*) De até 1.500 bytes para outro host
na mesma rede. Uma série é dirigida por um discurso de seis-byte codificado para o firmware da sua rede Ethernet carteira de trabalho de interface (NIC). Esses endereços são normalmente escritos como uma seqüência de números de dois dígitos hexadecimais separados
por dois pontos, como no *aa: bb: cc: ee: ff dd*.

Um quadro enviado por uma estação é visto por todas as estações conectadas, mas apenas o host de destino na verdade, o pega e processa. Se duas estações tentar enviar ao mesmo tempo, um *colisão* ocorre. Colisões em uma rede Ethernet são detectados muito rapidamente pelo sistema eletrônico das placas de interface e são resolvidos pelas duas estações de abortar a enviar, a cada espera um intervalo aleatório e de tentar novamente a transmissão. Você vai ouvir muitas histórias sobre colisões em Ethernet a ser um problema e que a utilização de redes Ethernet é de apenas cerca de 30 por cento da largura de banda disponível

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

por causa deles. Colisões em Ethernet são um *normal* fenômeno, e em uma rede Ethernet muito ocupado você não deve ficar surpreso ao ver as taxas de colisão de até cerca de 30 por cento. Utilização de redes Ethernet é mais realisticamente limitado a cerca de 60 por cento antes de precisar começar a se preocupar com isso.[7]

7 O FAQ Ethernet na http://www.faqs.org/faqs/LANs/ethernet-faq/ fala sobre este assunto, e uma riqueza de histórico detalhado e técnico informações estão disponíveis no web Charles Spurgeon Ethernet no site http://wwwhost.ots.utexas.edu/ethernet/.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Outros tipos de Hardware

Em instalações maiores, como Groucho Marx Universidade, Ethernet normalmente não é o único tipo de equipamento utilizado. Há muitos outros meios de comunicação de dados protocolos disponíveis e em uso. Todos os protocolos são listados suportados pelo Linux, mas devido a restrições de espaço, vamos descrevê-las brevemente. Muitos dos protocolos têm documentos HOWTO que os descrevem em detalhes, por isso você deve se referir àqueles se você estiver interessado em explorar aqueles que não descrevemos neste livro.

Na Universidade de Groucho Marx, LAN de cada departamento está ligado ao campus de rede "backbone" de alta velocidade, que é um cabo de fibra óptica que uma tecnologia de rede chamada *Fiber Distributed Data Interface* (FDDI). FDDI utiliza uma abordagem completamente diferente para a transmissão de dados, que basicamente envolve o envio de cerca de uma série de
tokens, Com uma estação de serem autorizados a enviar um quadro só se capta um sinal. A principal vantagem de um token passando protocolo é uma redução nas colisões. Portanto, o protocolo pode mais facilmente atingir a velocidade total do meio de transmissão de até 100 Mbps no caso do FDDI. FDDI, sendo baseada em fibra óptica, oferece um signifi- vantagem não pode porque o seu comprimento máximo do cabo é muito maior do que as tecnologias baseadas em fios. Tem limites de
até cerca de 200 km, o que o torna ideal para a ligação de muitos edifícios na cidade, ou como no caso da GMU, muitos prédios em um campus.

Da mesma forma, se houver qualquer equipamento de computação IBM ao redor, um IBM rede Token Ring é muito provável

que seja
instalado. Token Ring é usado como uma alternativa para Ethernet LAN em alguns ambientes, e oferece o mesmo tipo vantagens como FDDI em termos de alcançar velocidade total, mas em velocidades mais baixas (4 Mbps ou 16 Mbps), e menor custo, porque se baseia no fio ao invés de fibra. No Linux, redes Token Ring é configurado em quase precisamente da mesma maneira como a Ethernet, por isso não cobri-lo especificamente.

Embora seja muito menos provável hoje do que no passado, as tecnologias de LAN, tais como ArcNet e DECNet, pode ser instalado. O Linux suporta estes também, mas não cobri-los aqui.

Muitas redes nacionais operados por empresas de telecomunicações suportam os protocolos de comutação de pacotes. Provavelmente o mais popular destes é um padrão chamado X.25. Muitas redes públicas de dados, como Tymnet na EUA, Austpac na Austrália, e Datex-P na Alemanha oferecem este serviço. X.25 define um conjunto de redes proto- cols que descreve como equipamento terminal de dados, como um anfitrião, se comunica com a comunicação de dados equipamentos (um switch X.25). X.25 exige uma ligação de dados síncrona e, portanto, porta serial síncrona especiais hardware. É possível utilizar X.25 normal com portas seriais, se você usar um dispositivo especial chamado um PAD (Packet Montador Disassembler). O PAD é um dispositivo independente que fornece assíncrona portas seriais e uma syn- chronous porta serial. Ele gerencia o protocolo X.25 para que os dispositivos terminais simples podem fazer e aceitar X.25 conexões. X.25 é freqüentemente usado para transportar outros protocolos de rede, como TCP / IP. Desde datagramas IP não pode
simplesmente ser mapeado em X.25 (ou vice-versa), eles são encapsulados em pacotes X.25 e enviados pela rede. Existe uma implementação experimental do protocolo X.25 disponível para Linux.

Um protocolo mais recente, comumente oferecidos por empresas de telecomunicações é chamado *Frame Relay*. O Frame Relay partes protocolo uma série de recursos técnicos com o protocolo X.25, mas é muito mais parecido com o proto-IP col de comportamento. Assim como no X.25, Frame Relay requer um hardware especial síncrona serial. Devido à sua seme- laços, muitas cartas de apoio estes dois protocolos. Uma alternativa disponível que não requer nenhum interno especial hardware, mais uma vez contando com um dispositivo externo chamado de Frame Relay Access Device (FRAD) para gerenciar o en-
encapsulamento de pacotes Ethernet em pacotes Frame Relay para a transmissão em uma rede. Frame Relay é ideal para o transporte de TCP / IP entre sites. O Linux possui drivers compatíveis com alguns tipos de internos Frame Relay dispositivos.

Se você precisa de rede de maior velocidade que pode levar muitos tipos diferentes de dados, como voz digitalizada e vídeo, juntamente com seus dados de costume, ATM (Asynchronous Transfer Mode) é provavelmente o que você vai estar interessado em
ATM é uma tecnologia nova rede que foi projetado especificamente para proporcionar uma gerenciável, de alta velocidade, baixa latência meios de transporte de dados e fornecer controle sobre a qualidade de serviço (QS). Muitos tele- cátions empresas estão implantando infra-estrutura de rede ATM, pois permite a convergência de uma série de diferentes serviços de rede em uma plataforma, na esperança de conseguir uma poupança nos custos de gerenciamento e suporte. ATM é freqüentemente utilizado para o transporte TCP / IP. O Networking HOWTO oferece informações sobre o suporte para Linux disponível
para a ATM.

Freqüentemente, os radioamadores usam seus equipamentos de rádio para a rede de seus computadores, o que é comumente

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

chamado *pacote*
rádio. Um dos protocolos usados por operadores de rádio amador é chamado AX.25 e é vagamente derivada de X.25. operadores de rádio amadores utilizam o protocolo AX.25 para realizar TCP / IP e outros protocolos também. AX.25, como X.25,
requer hardware serial capaz de operação em sincronismo, ou um dispositivo externo chamado de "Terminal Node Con-Troller "para converter pacotes transmitidos através de uma ligação assíncrona serial em pacotes transmitidos de forma síncrona.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Há uma variedade de diferentes tipos de placas disponíveis para apoiar a operação de rádio por pacotes, estes

cartões
são geralmente referidos como sendo "Z8530 SCC base", e são nomeados após o mais popular tipo de comunicações controlador usado nos projetos. Dois dos outros protocolos que são comumente realizadas por AX.25 são os NetRom Rose e protocolos, que são protocolos de camada de rede. Uma vez que estes protocolos AX.25 atropelado, eles ter os requisitos de hardware mesmo. O Linux suporta uma aplicação inteiramente caracterizada do AX.25, NetRom, e protocolos de Rose. O AX25-HOWTO é uma boa fonte de informações sobre a aplicação destas Linux protocolos.

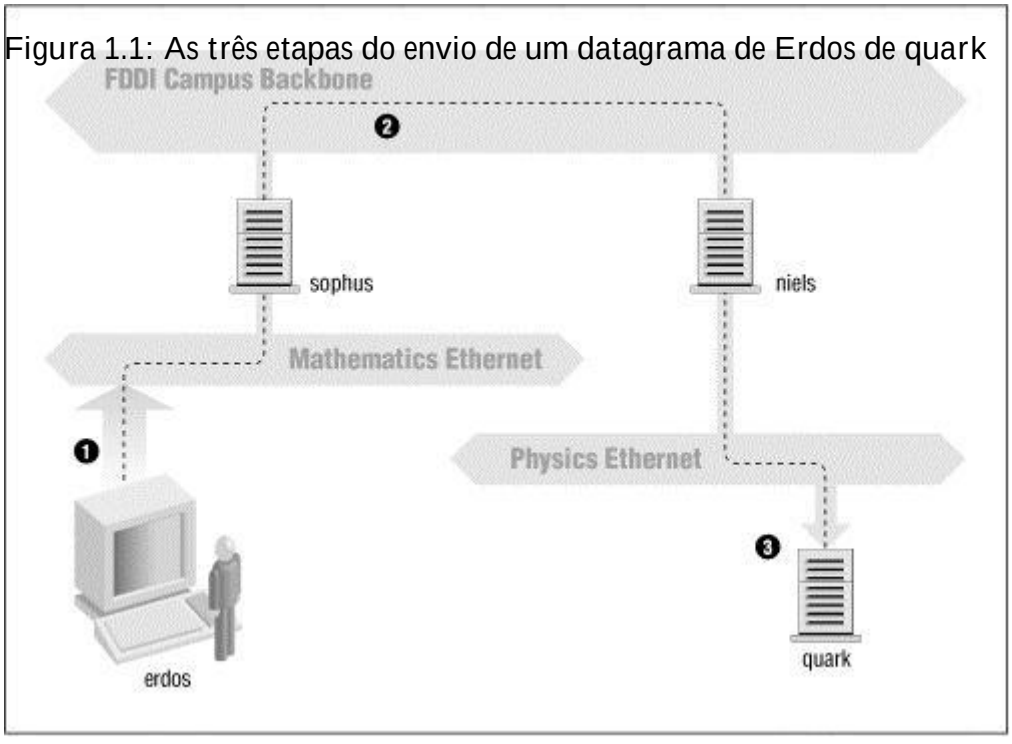
Outros tipos de acesso à Internet envolve a marcação de um sistema central mais lento, mas baratos linhas seriais (telefone, ISDN, e assim por diante). Estes exigem ainda um outro protocolo para transmissão de pacotes, como o SLIP ou PPP, que será descrito mais tarde.

O Protocolo de Internet

É claro que você não gostaria que sua rede seja limitado a uma Ethernet ou um ponto para apontar a ligação de dados. Idealiado, você gostaria de ser capaz de comunicar com um computador host, independentemente de qual tipo de físico-net trabalho que está conectado. Por exemplo, em instalações maiores, como Groucho Marx Universidade, que normalmente têm uma série de redes separadas que têm de ser ligados de alguma forma. No GMU, o departamento de Matemática executa duas Ethernets: um com máquinas velozes para os professores e diplomados, e outro com máquinas lentas para os alunos. Ambos são ligados à rede de backbone de campus FDDI.

Esta conexão é feita por um servidor dedicado chamado *gateway* que manipula os pacotes de entrada e saída de copiá-las entre as duas redes Ethernet e um cabo de fibra óptica FDDI. Por exemplo, se você está na Matemática departamento e deseja acessar *quark* na rede do departamento de Física da sua caixa de Linux, a rede software não irá enviar pacotes para *quark* diretamente porque ele não está na mesma rede. Portanto, ele tem que confiar sobre a porta de entrada para atuar como um encaminhador. O gateway (nomeado *sophus*) Encaminha esses pacotes para o seu portão peer-
forma *niels* no Departamento de Física, utilizando a rede backbone, com *niels* entregá-lo ao destino machine. Fluxo de dados entre *Erdos* e *quark* é mostrado na Figura 1.1.

Figura 1.1: As três etapas do envio de um datagrama de Erdos de quark



PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Este esquema de direcionar os dados para um host remoto é chamado *roteamento*, E os pacotes são muitas vezes referida como *datagramas* em
neste contexto. Para facilitar as coisas, a troca de datagramas é regida por um protocolo único que é independente da hardware utilizado: IP, ou *Protocolo da Internet*. No capítulo 2, *Problemas de rede TCP / IP*, Vamos cobrir IP eo problemas de roteamento em maior detalhe.

O principal benefício do IP é que ele transforma redes fisicamente diferentes em uma rede aparentemente homogénea. Isso é chamado de internetworking, e da consequente "meta-rede" é chamado de *Internet*. Note a sutil diferença aqui entre *um* Internet e *o* Internet. O último é o nome oficial de uma internet especial global.

Claro, a IP também requer um esquema de endereçamento independente do hardware. Isto é conseguido através da atribuição de

cada um host
número de 32 bits exclusivo chamado *endereço IP*. Um endereço IP é normalmente escritos como quatro números decimais, um para
cada porção de 8 bits, separados por pontos. Por exemplo, *quark* pode ter um endereço IP *0x954C0C04*, Que seria escrito como *149.76.12.4*. Esse formato também é chamado *notação decimal* e, às vezes *dotted quad notação*. É cada vez mais indo sob o nome de IPv4 (Internet Protocol, versão 4) por um novo padrão
Chamado IPv6 oferece muito mais flexibilidade de endereçamento, bem como outras características modernas. Será, no mínimo, um ano depois
o lançamento desta edição antes IPv6 está em uso.

Você vai notar que agora temos três tipos de endereços: primeiro, há o nome do host, como *quark*,
depois há os endereços IP e, finalmente, há endereços de hardware, como o endereço Ethernet de 6 bytes. Todas essas Endereços de alguma forma tem de corresponder de modo que quando você digita `quark rlogin`, O software de rede pode ser
dada *quark*"Endereço IP, e quando IP fornece todos os dados Ethernet para o Departamento de Física, ela de alguma forma tem que
descobrir o endereço Ethernet correspondente ao endereço IP.

Nós vamos lidar com estas situações no Capítulo 2. Por ora, basta lembrar que estes passos de encontrar
endereços são chamados *resolução de nomes*, Para o mapeamento de nomes de máquinas em endereços IP e *resolução de endereços*, Para
mapear o último a endereços de hardware.

IP sobre linhas seriais

Nas linhas de série, um "de facto" existe padrão conhecido como SLIP, ou *Serial Line IP*. A modificação do SLIP conhecido

como
CSLIP, ou *SLIP comprimido*, Realiza a compressão do cabeçalho IP para fazer melhor uso da banda relativamente baixa largura prevista pela maioria dos links seriais. Outro protocolo serial PPP ou a *Protocolo Ponto-a-Ponto*. O PPP é mais moderna do que SLIP e inclui uma série de características que o tornam mais atraentes. Sua principal vantagem em relação ao SLIP
é que não se limita a transportar datagramas IP, mas é projetado para permitir que apenas sobre todo o protocolo a ser realizado através dele.

O Transmission Control Protocol

Envio de datagramas de um host para outro não é toda a história. Se você efetuar login em *quark*, Você quer ter uma
ligação segura entre o seu `rlogin` processo em *Erdos* e processar o shell na *quark*. Assim, a infor-
ção enviados para cá e para lá devem ser divididas em pacotes pelo emissor e remontados em um fluxo de caracteres pela receptor. Trivial quanto parece, isso envolve uma série de tarefas complicadas.

Uma coisa muito importante saber sobre IP é que, pela intenção, não é confiável. Suponha que dez pessoas no seu
Ethernet começou a baixar a última versão do código-fonte do Netscape web browser a partir do servidor FTP da GMU. A quantidade de tráfego gerado pode ser demais para o gateway de lidar, porque é muito lento e é apertado
na memória. Agora, se acontecer de você enviar um pacote para *quark*,*sophus* pode estar fora do espaço do buffer por um momento e
portanto, incapaz de transmiti-lo. IP resolve este problema simplesmente descartá-lo. O pacote é perdido. É portanto, a responsabilidade de comunicar os anfitriões para verificar a integridade ea integridade dos dados e retransmitir, em caso de erro.

Este processo é realizado por ainda outro protocolo, *Transmission Control Protocol* (TCP), que constrói uma confiança

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

serviço em cima de IP. A propriedade essencial do TCP é que ele usa o IP para lhe dar a ilusão de uma conexão simples
ção entre os dois processos em seu host ea máquina remota, então você não precisa se preocupar sobre como e
percurso ao longo do qual os dados realmente viaja. Uma conexão TCP funciona essencialmente como um tubo de duas vias que tanto
processos podem escrever e ler. Pense nisso como uma conversa telefônica.

TCP identifica os pontos finais de uma conexão pelo endereço IP dos dois hosts envolvidos eo número
de um *porto* em cada host. As portas podem ser vistos como pontos de fixação para conexões de rede. Se quisermos, a tensão
exemplo do telefone um pouco mais, e você imagina que as cidades são como anfitriões, pode-se comparar os endereços IP para

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

códigos de área (onde os números mapa para cidades), e números de porta para os códigos locais (onde os números mapa para individual
pessoas, telefones). Um host indivíduo pode suportar muitos serviços diferentes, cada um caracterizado por seu próprio porto número.

Na `rlogin` exemplo, o aplicativo cliente (`rlogin`) Abre uma porta no *Erdos* e se conecta à porta 513 no *quark*, Ao qual o `rlogind` servidor é conhecido para ouvir. Essa ação estabelece uma conexão TCP. Usando este conexão, `rlogind` executa o procedimento de autorização e, em seguida, gera o shell. O shell padrão
entrada e saída são redirecionados para a conexão TCP, de modo que qualquer coisa que você escreva para `rlogin` em sua máquina
serão passadas através do fluxo TCP e ser dada para o shell como entrada padrão.

O User Datagram Protocol

Claro, o TCP não é o protocolo do usuário somente em redes TCP / IP. Embora adequado para aplicações como `rlogin`, A sobrecarga envolvida é proibitivo para aplicações como o NFS, que em vez usa um protocolo irmão do Chamado TCP UDP, ou *User Datagram Protocol*. Assim como TCP, UDP permite que um aplicativo para manter contato com um serviço em
uma determinada porta da máquina remota, mas não estabelece uma conexão para isso. Em vez disso, use-o para enviar pacotes individuais para o serviço de destino - daí o seu nome.

Suponha que você deseja solicitar uma pequena quantidade de dados de um servidor de banco de dados. Leva pelo menos três datagramas
estabelecer uma conexão TCP, mais três para enviar e confirmar uma pequena quantidade de dados em cada sentido, e outro três para fechar a conexão. UDP fornece-nos um meio de usar apenas dois datagramas para atingir quase o mesmo resultado. UDP é considerado sem conexão, e não nos obrigam a criar e encerrar uma sessão. Nós sim-
ply colocar nossos dados em um datagrama e enviá-lo para o servidor, o servidor formular sua resposta, coloca os dados em um datagrama dirigida de volta para nós, e transmite-lo de volta. Embora isso seja mais rápido e mais eficiente que o TCP para operações simples, UDP não foi projetado para lidar com a perda de datagrama. Cabe ao aplicativo, um servidor de nomes por exemplo, para cuidar disso.

Mais de Portos

As portas podem ser vistos como pontos de fixação para conexões de rede. Se um aplicativo quer oferecer um certo serviços, atribui-se a uma porta e espera por clientes (isto é também chamado *Acesse* na porta). Um cliente que quer usar este serviço aloca uma porta na sua máquina local e conecta-se a porta do servidor no host remoto.
A mesma porta pode ser aberta, muitas máquinas diferentes, mas em cada máquina, apenas um processo pode abrir uma porta a qualquer momento.

Uma propriedade importante dos portos é que, uma vez que uma conexão foi estabelecida entre o cliente eo servidor, outra cópia do servidor pode acompanhar a porta do servidor e escute mais clientes. Esta propriedade permite, por exemplo, vários logins simultâneos remoto para o mesmo host, todos usando a mesma porta 513. O TCP é capaz de dizer a esses conexões entre si porque todos eles vêm de diferentes portos ou hosts. Por exemplo, se você log in
duas vezes para *quark* a partir de *Erdos*, O primeiro `rlogin` cliente irá utilizar a porta local 1023, eo segundo usará a porta 1022. Ambos, porém, irá se conectar à mesma porta 513 no *quark*. As duas conexões vão ser distinguidos pela utilização de números de porta usados em *Erdos*.

Este exemplo mostra a utilização de portos como pontos de encontro, onde um cliente contata uma porta específica para obter uma
serviço específico. Para que um cliente para saber o número da porta apropriado, um acordo deve ser alcançado entre os administradores de ambos os sistemas na atribuição destes números. Para os serviços que são amplamente utilizados, tais como
`rlogin`, Estes números têm que ser administrados de forma centralizada. Isso é feito pelo IETF (Internet Engineering Task Force), que regularmente lança um chamado RFC *Assigned Numbers* (RFC-1700). Ele descreve, entre outras coisas, os números de porta atribuído aos serviços bem conhecidos. Linux utiliza um arquivo chamado */ Etc / services* que mapeia os nomes de serviço
em números.

É interessante notar que, embora ambas as conexões TCP e UDP dependem de portas, esses números não entram em conflito. Isto significa que a porta TCP 513, por exemplo, é diferente da porta UDP 513. Na verdade, essas portas servem como acesso aponta para dois serviços diferentes, a saber `rlogin` (TCP) e `rwho` (UDP).

PDF Creator - PDF 4Free v2.0 http://www.pdf4free.com

A Biblioteca de Socket

Nos sistemas operacionais Unix, o software de executar todas as tarefas e protocolos descritos acima são geralmente parte de o kernel, e assim é em Linux. A interface de programação mais comuns no mundo Unix é o *Berkeley*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Socket Library. Seu nome deriva de uma analogia popular que vê as portas, tomadas e se conectar a uma porta como conectar dentro Ele fornece a *vincular* chamada para especificar um host remoto, um protocolo de transporte, e um serviço que um programa
Pode ligar ou ouvir (usando *contato*,*ouvir*E *aceitar*). A biblioteca do soquete é um pouco mais geral na medida em que oferece não apenas uma classe de soquetes TCP / IP-based (o *AF_INET* slots), mas também uma classe que manipula conexões locais para a máquina (o *AF_UNIX* classe). Algumas implementações também pode lidar com outras classes, como a XNS (*Xerox do Sistema de Rede*) Ou protocolo X.25.

No Linux, a biblioteca do soquete é parte do padrão *libc* biblioteca C. Ele suporta os *AF_INET* e *AF_INET6* soquetes para TCP / IP e *AF_UNIX* para soquetes de domínio Unix. Ele também suporta *AF_IPX* para protocolos de rede Novell, *AF_X25* para o protocolo de rede X.25, *AF_ATMPVC* e *AF_ATMSVC* para o protocolo de rede ATM e *AF_AX25*,*AF_NETROM*E *AF_ROSE* soquetes para suporte de protocolo de rádio amador. Outras famílias de protocolos estão sendo desenvolvidos e serão adicionadas no tempo.

UUCP Networks

Unix-to-Unix Copy (UUCP) começou como um pacote de programas que os arquivos transferidos através de linhas seriais,

sched-
uled essas transferências, e iniciou a execução de programas em locais remotos. Ela tem sofrido grandes mudanças desde sua primeira implementação em finais dos anos setenta, mas ainda é bastante espartano nos serviços que oferece. Sua aplicação principal-
ção ainda está em Wide Area Networks, baseada em ligações telefônicas periódicas discada.

UUCP foi desenvolvido inicialmente pela Bell Laboratories em 1977 para a comunicação entre o seu desenvolvimento Unix sites. Em meados de 1978, esta rede já está ligado mais de 80 sites. Ele estava correndo como um aplicativo de e-mail, bem como impressão remota. Entretanto, o uso central do sistema foi na distribuição de novos softwares e correções de bugs. Hoje, UUCP não se limita apenas ao ambiente Unix. Há portos livres e comerciais disponíveis para uma vari-
ciedade de plataformas, incluindo AmigaOS, DOS e Atari TOS.

Uma das principais desvantagens das redes UUCP é que eles operam em lotes. Ao invés de ter uma per-
conexão permanente estabelecida entre os hosts, ele usa conexões temporárias. Uma máquina host UUCP pode discar para outro host UUCP apenas uma vez por dia, e apenas por um curto período de tempo. Quando for ligado, ele vai transferência de todas as notícias, e-mail e arquivos que tenham sido colocadas em fila e, em seguida desligue. É esta filas que limita
os tipos de aplicativos que UUCP pode ser aplicado. No caso de e-mail, o usuário pode preparar uma mensagem de e-mail e postá-lo. A mensagem vai permanecer na fila na máquina UUCP até que ele disca para outro host UUCP para transferir a mensagem. Isso é bom para os serviços de rede, tais como e-mail, mas não serve para todos para serviços como `rlogin`.

Apesar dessas limitações, existem ainda muitas redes UUCP que operam em todo o mundo, principalmente por correr hob-
byists, que oferecem acesso à rede privada de usuários, a preços razoáveis. A principal razão para o antigo popular-
dade de UUCP é que era muito barato comparado a ter seu computador conectado diretamente à Internet. Para tornar o computador um nó UUCP, tudo que você precisava era de um modem, um trabalho de implementação UUCP, e outro UUCP nó que estava disposta a alimentá-lo e-mail e notícias. Muitas pessoas estavam preparadas para prover UUCP feeds indivíduos, porque essas ligações não colocar muita demanda em sua rede existente.

Nós cobrimos a configuração do UUCP em um capítulo próprio no final do livro, mas não vamos focar nisso também heav-
lia, como ela está sendo substituída rapidamente com o TCP / IP, já que acesso barato à Internet tornou-se normalmente disponíveis em
maior parte do mundo.

Redes Linux

Como é o resultado de um esforço concertado de programadores ao redor do mundo, o Linux não teria sido possível sem a rede mundial. Portanto, não é surpreendente que, nos estágios iniciais de desenvolvimento, várias pessoas começaram para trabalhar em fornecê-lo com recursos de rede. Uma implementação UUCP foi rodando no Linux praticamente desde o início, e trabalhar em redes TCP / IP-based começou por volta do Outono de 1992, quando Ross Biro e outros criaram o que agora se tornou conhecido como Net-1.

Depois de encerrar o desenvolvimento ativo Ross maio 1993, Fred van Kempen começou a trabalhar em uma nova

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

implementação,
reescrever grandes partes do código. Este projeto ficou conhecido como Net-2. A primeira versão pública, Net-2d, foi feita em No verão de 1993 (como parte do kernel 0.99.10), e desde então tem sido mantido e ampliado por várias pes-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

soas, principalmente Alan Cox.[8] Atrabalho original de lan era conhecido como Net-2Debugged. Após a depuração pesados e
inúmeras melhorias ao código, ele mudou seu nome para Net-3 após Linux 1.0 foi lançado. O código-3 Net foi desenvolvido para Linux 1.2 e Linux 2.0. Os kernels 2.2 e posterior utilização da rede versão Net-4 suporte, que continua a ser a oferta padrão oficial hoje.

O Net-4 código Linux Network oferece uma grande variedade de drivers de dispositivos e recursos avançados. Standard Net-4 protocolos incluem SLIP e PPP (para o envio de tráfego de rede através de linhas de série), PLIP (por linhas paralelas), IPX (para
redes Novell compatíveis, que discutiremos no Capítulo 15, *IPX eo sistema de arquivos NCP*), AppleTalk (para redes da Apple) e AX.25, NetRom e Rose (para as redes de rádio amador). Outros padrão Net-4 possui incluem firewall IP, IP Contabilidade (discutido mais adiante no Capítulo 9, *Firewall TCP / IP* e Capítulo 10, *Conta-IP ing*) E IP Masquerade (discutido posteriormente no Capítulo 11, *IP Masquerade e Network Address Translation*. IP tunelamento em um par de diferentes sabores e política de recursos avançados de roteamento são suportados. Uma variedade muito grande de
dispositivos Ethernet com suporte, além de suporte para alguns FDDI, Token Ring, Frame Relay e ISDN, e cartões ATM.

Além disso, há uma série de outras funcionalidades que melhoram muito a flexibilidade do Linux. Estas características Incluímos uma implementação do sistema de arquivos SMB, que interage com aplicações como *LanManager* e Microsoft Windows, chamado Samba, escrita por Andrew Tridgell, e uma implementação do NCP Novell (Protocolo Core NetWare).[9]

Listras diferentes de desenvolvimento

Houve, por diversas vezes, variando os esforços de desenvolvimento de rede activa para Linux.

Fred continuou desenvolvimento após Net-2Debugged foi feita a implementação da rede oficial. Este desenvol-desenvolvimento levou à Net-2e, que contou com um design muito revista da camada de rede. Fred estava trabalhando para-ala padronizado Device Driver Interface (DDI), mas o trabalho Net-2e terminou agora.

Contudo uma outra implementação de redes TCP / IP veio de Matthias Urlichs, que escreveu um driver para ISDN Linux e FreeBSD. Para este driver, ele integrou uma parte do código BSD rede no kernel do Linux. Isso projeto, também não está sendo trabalhado.

Tem havido uma série de mudanças rápidas na implementação de rede do kernel do Linux, ea mudança é ainda o como lema o desenvolvimento continua. Às vezes, isso significa que as mudanças também têm de ocorrer em outros softwares, tais como as ferramentas de configuração de rede. Enquanto isso não é mais tão grande um problema quanto era uma vez, você ainda pode
achar que atualizar o seu kernel para uma versão posterior significa que você deve atualizar suas ferramentas de configuração de rede,
também. Felizmente, com o grande número de distribuições do Linux disponíveis atualmente, esta é uma tarefa muito simples.

A implementação da rede Net-4 já está bastante madura e está em uso em um número muito grande de sites ao redor do mundo. Muito trabalho tem sido feito na melhoria do desempenho da aplicação-4 líquido, e agora com-petes com as melhores implementações disponíveis para as plataformas de hardware mesmo. Linux está se proliferando na Internet Service Provider ambiente, e é frequentemente usada para construir, barato e seguro Mundo servidores Wide Web, servidores de correio e servidores de notícias para estes tipos de organizações. Agora existe interesse suficiente em desenvolvimento
Linux que está conseguindo manter a par de tecnologia de rede, uma vez que as alterações e versões atuais do kernel do Linux oferecer a próxima geração do protocolo IP, IPv6, como uma oferta padrão.

Onde Obter o Código

Parece estranho agora para lembrar que nos primeiros dias do desenvolvimento de código de rede do Linux, o kernel padrão necessário um kit de remendo enorme para adicionar o suporte de rede para ele. Hoje, o desenvolvimento da rede ocorre como parte do
mainstream processo de desenvolvimento do kernel Linux. O último Linux kernel estável pode ser encontrada em ftp.kernel.org em
/ Pub/linux/kernel/v2.x /, Onde *x* é um número par. O último kernels experimentais Linux podem ser encontrados no ftp.kernel.org em */ Pub/linux/kernel/v2.y /*, Onde *y* é um número ímpar. Há espelhos fonte do Linux kernel todos todo o mundo. Agora, é difícil imaginar o Linux sem suporte de rede padrão.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

8 Alan pode ser alcançado em alan@lxorguk.ukuu.org.uk
9 NCP é o protocolo em que a Novell arquivo e serviços de impressão são baseados

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Manutenção do sistema

Ao longo deste livro, vamos lidar principalmente com problemas de instalação e configuração. Administração é, como-
nunca, muito mais do que isso - depois de configurar um serviço, você tem que mantê-lo funcionando, também. Para a maioria dos serviços, mas apenas um
atendimento pouco vai ser necessário, enquanto alguns, como o correio e notícias, exigem que você execute tarefas de rotina para
manter seu sistema atualizado. Vamos discutir essas tarefas em capítulos posteriores.

O mínimo absoluto de manutenção é a verificação do sistema e arquivos de log por aplicação regular de condições de erro
ções e eventos incomuns. Muitas vezes, você vai querer fazer isso por escrito um par de shell scripts administrativos e executá-los periodicamente a partir de `cron`. As distribuições fonte de algumas aplicações importantes, como `estalagem` Notícias ou C,
contêm tais scripts. Você só tem que adaptá-los às suas necessidades e preferências.

A saída de qualquer um dos seus `cron` trabalhos devem ser enviados para uma conta administrativa. Por padrão, a pedido de

muitos
cátions vai enviar relatórios de erros, estatísticas de uso, ou resumos de log para o arquivo *root* consideração. Isso só faz sentido Se você fizer login como *root* freqüentemente, uma idéia muito melhor é para a frente *root*'S-mail para sua conta pessoal, definindo
um alias de correio, conforme descrito no Capítulo 19, *Obter Exim Funcionando* ou do Capítulo 18, *Sendmail*.

No entanto cuidado você configurou o seu site, garantias lei de Murphy que algum problema *vai* superfície plana,
tualmente. Assim, a manutenção de um sistema também significa estar disponível para denúncias. Normalmente, as pessoas esperam que
o administrador do sistema pode ao menos ser contatado por e-mail como root, mas há também outros endereços que são comumente utilizado para alcançar a pessoa responsável por um aspecto específico de manutenção. Por exemplo, as queixas sobre uma configuração de correio funcionando normalmente será dirigida ao postmaster, e problemas com a notícia sistema pode ser comunicada ao newsmaster ou usenet. E-mail para hostmaster deve ser redirecionada para a pessoa responsável dos serviços de acolhimento da rede básica e serviço de nomes DNS, se você executar um servidor de nomes.

Sistema de Segurança

Outro aspecto muito importante da administração de sistemas em ambiente de rede está a proteger seu sistema e
usuários de intrusos. Carelessly sistemas gerenciados oferecem às pessoas mal-intencionados muitas metas. Os ataques variam de
adivinhação de senha para Ethernet snooping, e os danos causados podem variar de mensagens de correio falsificou dados perda ou violação da privacidade de seus usuários. Vamos citar alguns problemas particulares quando se discute o contexto em que podem ocorrer e algumas defesas comuns contra eles.

Esta seção discutirá alguns exemplos e técnicas básicas para lidar com a segurança do sistema. É claro que o
temas abordados não pode tratar todos os problemas de segurança que pode ser enfrentado em detalhes, pois eles servem apenas para ilustrar o
problemas que possam surgir. Portanto, ler um bom livro sobre segurança é uma necessidade absoluta, especialmente em um líquido,
trabalhou sistema.

Sistema de segurança começa com a administração do sistema bom. Isto inclui a verificação da propriedade e as permissões
de todos os arquivos vitais e diretórios e usar o monitoramento de contas privilegiadas. O programa COPS, por exemplo, vai verificar o seu sistema de arquivos e arquivos de configuração comum para as permissões de invulgar ou outras anomalias. É também
aconselhável utilizar um conjunto de senha que impõe certas regras de senhas dos usuários que os tornam difíceis de adivinhar. O conjunto de senhas sombras, por exemplo, requer uma senha para ter pelo menos cinco cartas e contêm
maiúsculas e minúsculas e números, bem como caracteres não-alfabéticos.

Ao fazer um serviço de acesso à rede, certifique-se de dar-lhe "privilégio mínimo", não permitem que ele faça
coisas que não são necessários para que ele funcione como projetado. Por exemplo, você deve fazer programas setuid para *root* ou
algum outro privilegiado somente quando necessário. Além disso, se você quiser usar um serviço para apenas um número muito limitado
pedido, não hesite em configurá-lo de forma tão restritiva como a sua aplicação especial permite. Por exemplo, se você deseja permitir que os hosts sem disco de boot de sua máquina, você deve fornecer *Trivial File Transfer Protocol* (TFTP)
para que possam baixar os arquivos de configuração básica do */ Boot* diretório. No entanto, quando usado unrestric-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

respectivamente, TFTP permite que os usuários em qualquer lugar do mundo para fazer download de qualquer arquivo lido a partir do seu sistema. Se isso
não é o que você quer, restringir TFTP serviço à */ Boot* Diretório.[10]

Você também pode querer restringir determinados serviços para usuários de certos hosts, digamos, de sua rede local. Em Capítulo 12, apresentamos `tcpd`, Que faz isso para uma variedade de aplicações de rede. métodos mais sofisticados, ods de restringir o acesso a hosts ou serviços específicos será explorada mais adiante no Capítulo 9.

10 Voltaremos a este tema no capítulo 12, *Rede Características importantes*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Outro ponto importante é evitar o software "perigoso". É claro que qualquer software que você utiliza podem ser perigosos
porque o software pode ter bugs que pessoas inteligentes podem explorar para obter acesso ao seu sistema. Coisas como esta acontecer, e não há proteção completa contra ele. Esse problema afeta o software livre e comercial produtos semelhantes.[11] No entanto, os programas que requerem privilégios especiais são inerentemente mais perigosos que outros, porque
qualquer falha pode ter conseqüências drásticas.[12] Se você instalar um programa setuid para efeitos de rede, ser duplamente o cuidado de verificar a documentação para que você não cria uma brecha de segurança por acidente.

Outra fonte de preocupação deve ser os programas que permitem a execução de login ou de comando com autenticaç limitadoção. A `rlogin`,`rsh`E `rexec` todos os comandos são muito úteis, mas oferecer autenticação muito limitada da chamando partido. A autenticação é baseada na confiança do nome do host chamando obtidos a partir de um servidor de nomes (falaremos
sobre isso mais tarde), que pode ser falsificado. Hoje ele deve ser uma prática habitual para desativar o `r` com comandos decompletamente e substituí-los com o `ssh` conjunto de ferramentas. A `ssh` ferramentas de usar uma autenticação mais confiável método e prestação de outros serviços, tais como encriptação e compactação, bem como.

Você nunca pode descartar a possibilidade de que as suas precauções pode falhar, independentemente de quão cuidadoso você ter sido.
Você deve, portanto, certifique-se de detectar intrusos cedo. Verificando os arquivos de log do sistema é um bom ponto de partida,
mas o intruso provavelmente é inteligente o bastante para prever esta ação e irá apagar todos os traços óbvio que ele ou ela esquerda. No entanto, existem ferramentas como `tripwire`, Escrito por Gene Kim e Gene Spafford, que permitem verificar sistema de arquivos vitais para ver se o seu conteúdo ou permissões foram alteradas. `tripwire` calcula forte diversos checksums sobre estes arquivos e os armazena em um banco de dados. Durante as corridas subsequentes, as somas são recoputed e comparados com os armazenados para detectar qualquer modificação.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

11 Houve sistemas comerciais Unix (que você tem que pagar muito dinheiro para) que veio com um setuid-*root* shell script, que usuários autorizados a ganhar *root* privilégio usando um simples truque padrão

12 Em 1988, o worm RTM trouxe grande parte da Internet parar de funcionar, em parte através da exploração de um buraco em alguns programas, incluindo o `sendmail` programa. Este buraco há muito tempo já foi corrigido

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 2 - Questões de rede TCP / IP

Neste capítulo, voltamo-nos para as decisões de configuração que você precisará fazer ao ligar sua máquina Linux a uma rede TCP / IP, incluindo lidar com endereços IP, nomes de máquinas e problemas de roteamento. Este capítulo dá-lhe o fundo que você precisa para entender o que sua configuração exige, enquanto os capítulos seguintes cobrem as ferramentas você irá usar.

Para saber mais sobre TCP / IP e as razões por trás disso, referem-se ao conjunto de três volumes *Internetworking com TCP / IP*, De Douglas R. Comer (Prentice Hall). Para um guia mais detalhado para gerenciar uma rede TCP / IP, consulte *TCP / IP Network Administration* por Craig Hunt (O'Reilly).

Interfaces de Rede

Para ocultar a diversidade de equipamentos que podem ser usados em um ambiente de rede, TCP / IP define um resumo *interface* através do qual o hardware é acessado. Essa interface oferece um conjunto de operações que é o mesmo para todos tipos de ofertas de hardware e, basicamente, com o envio e recebimento de pacotes.

Para cada dispositivo de rede periférica, uma interface de correspondente tem de estar presente no kernel. Por exemplo, interfaces Ethernet no Linux são chamados por nomes como *eth0* e *eth1*; PPP (discutido no Capítulo 8, *O ponto-Protocolo a-Ponto*) Interfaces são nomeadas *ppp0* e *ppp1*E interfaces FDDI são dados nomes como *fddi0* e *fddi1*. Esses nomes de interface são usados para fins de configuração quando você deseja especificar um físico particular dispositivo em um comando de configuração, e eles não têm nenhum significado além desse uso.

Antes de ser utilizado por redes TCP / IP, uma interface deve ser atribuído um endereço IP que lhe serve de identificação ao se comunicar com o resto do mundo. Este endereço é diferente do nome da interface homem-citadas anteriormente, se você comparar uma interface para uma porta, o endereço é como o crachá preso nele.

Outros parâmetros do dispositivo pode ser definido como o tamanho máximo de datagramas que podem ser processados por um determinado peça de hardware, que é conhecido como *Maximum Transfer Unit* (MTU). Outros atributos serão introduzidas mais tarde. Felizmente, a maioria dos atributos têm padrões razoáveis.

Endereços IP

Como mencionado no Capítulo 1, *Introdução às Redes*, O protocolo de rede IP compreende endereços como 32 - número de bits. Cada máquina deve ser atribuído um número único para o ambiente de rede.[13] Se você está de execução ning uma rede local que não tem o tráfego TCP / IP com outras redes, você pode atribuir esses números ac-cordões com suas preferências pessoais. Há algumas faixas de endereços IP que foram reservadas para essa privada redes. Esses intervalos são listados na Tabela 2.1.No entanto, para os sítios na Internet, os números são atribuídos por um autoridade central, o *Network Information Center* (NIC).[14]

Os endereços IP são divididos em quatro números de oito bits chamado *octetos* para facilitar a leitura. Por exemplo, *quark.physics.groucho.edu* tem um endereço IP *0x954C0C04*, Que é escrito como *149.76.12.4*. Esse formato é muitas vezes referida como *notação decimal com pontos*.

Outra razão para esta notação é que os endereços IP são divididos em um *rede* número, que está contido no levando octetos, e um *host* número, que é o resto. Ao aplicar a NIC de endereços IP, que são não atribuído um endereço para cada host único que você planeja usar. Em vez disso, você recebe um número de rede e al-podem confiar todos os endereços IP válidos dentro desta faixa para os hosts em sua rede de acordo com suas preferências.

---

13 A versão do protocolo Internet mais utilizado na Internet é a versão 4. Um grande esforço tem sido dispendido na concepção de um substituição chamado IP versão 6. IPv6 utiliza um esquema diferente de endereçamento e endereços de maior dimensão. O Linux tem uma implementação do IPv6, mas ele não está pronto para documentá-lo neste livro ainda. O suporte do kernel Linux para o IPv6 é bom, mas um grande número de aplicações de rede precisa ser modificado para apoiá-lo também. Fique atento.

14 Freqüentemente, os endereços IP será atribuído pelo provedor de quem comprar a sua conectividade IP. No entanto, você também pode aplicar a NIC diretamente para um endereço IP para a sua rede através do envio de e-mail para hostmaster@internic.net, ou usando o formulário em http://www.internic.net/.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O tamanho da parte de host depende do tamanho da rede. Para acomodar as diferentes necessidades, de várias classes de redes, definindo lugares diferentes para dividir os endereços IP, foram definidos. As redes de classe são descritas aqui:

Classe A

Classe A é composto por redes *1.0.0.0* através *127.0.0.0*. O número de rede está contido no primeiro octeto. Essa classe fornece uma parte de host de 24 bits, permitindo que cerca de 1,6 milhões de hosts por
rede.

Classe B

Classe B contém redes *128.0.0.0* através *191.255.0.0*; O número de rede está em primeiro dois octetos. Esta classe permite 16.320 redes com 65.024 hosts cada.

Classe C

As redes classe C variam de *192.0.0.0* através *223.255.255.0*, Com o número da rede con-sustentado nos três primeiros octetos. Esta classe permite a quase 2 milhões de redes com até 254 hosts.

Classes D, E e F

Endereços de cair na faixa de *224.0.0.0* através *254.0.0.0* são experimentais ou são reservados para o uso para fins específicos e não especificam qualquer rede. IP Multicast, que é um serviço que permite que o material a ser transmitida para vários pontos em um Internet ao mesmo tempo, foi tão-assinado endereços dentro deste intervalo.

Se voltarmos ao exemplo do capítulo 1, vemos que *149.76.12.4*, O endereço do *quark*, Refere-se ao host *12.4* em a rede classe B *149.76.0.0*.

Você deve ter notado que nem todos os valores possíveis da lista anterior foram autorizadas para cada octeto na parte de host. Isso ocorre porque octetos *0* e *255* são reservados para propósitos especiais. Um endereço de onde todos os bits são parte de host 0 refere-se
à rede e um endereço onde todos os bits da parte de host são um é chamado de *endereço de broadcast*. Isto refere-se a todos os hosts da rede especificado simultaneamente. Assim, *149.76.255.255* não é um endereço de host válido, mas refere-se a todos os hosts na rede *149.76.0.0*.

Um número de endereços de rede são reservados para propósitos especiais. *0.0.0.0* e *127.0.0.0* dois endereços. O primeiro é chamado de *rota padrão*Eo último é o *endereço de loopback*. A rota padrão tem a ver com o rotas forma os datagramas IP.

Rede *127.0.0.0* está reservada para o tráfego IP local para o seu acolhimento. Normalmente, o endereço *127.0.0.1* será atribuído a um
interface especial no seu hospedeiro, o *interface de loopback*, Que age como um circuito fechado. Qualquer pacote IP entregue ao esta interface de TCP ou UDP será devolvida a eles como se tivesse acabado de chegar de alguma rede. Isso permite que você para desenvolver e testar o software de rede sem nunca usar uma rede "real". A rede loopback também permite a utilização de software de rede em uma máquina independente. Isto pode não ser tão incomum quanto parece, pois exemplo, muitos sites UUCP não tem conectividade IP de todo, mas ainda quer rodar o sistema de notícias INN. Para funcionamento no Linux, DCI requer a interface loopback.

Alguns intervalos de endereços de cada uma das classes de rede foram reservadas e designadas como "reservados" ou "privado" intervalos de endereços. Esses endereços são reservados para uso em redes privadas e não são roteados na Internet. Eles são comumente usadas por organizações de construção de sua própria intranet, mas até mesmo as redes pequenas, muitas vezes encontrá-los úteis.
Os endereços de rede reservados aparecer em Tabela 2.1.

Tabela 2.1: intervalos de endereços IP reservados para uso privado

Classe	Redes
A	10.0.0.0 até 10.255.255.255
B	172.16.0.0 até 172.31.0.0
C	192.168.0.0 até 192.168.255.0

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Address Resolution

Agora que você já viu como os endereços IP são compostos, você pode estar se perguntando como eles são usados em uma rede

Ethernet
ou rede Token Ring para abordar diferentes hospedeiros. Afinal, estes protocolos têm os seus próprios endereços para identificar hosts que não têm absolutamente nada em comum com um endereço IP, não é? Direita.

É necessário um mecanismo para mapear endereços IP para os endereços da rede subjacente. O mecanismo usado é o *Endereço Resolution Protocol* (ARP). Na verdade, ARP não se limita a Ethernet ou Token Ring, mas é usado em outros tipos de redes, tais como o protocolo AX.25 amadores de rádio. A ideia subjacente a ARP é exatamente o que a maioria das pessoas fazem quando têm de encontrar Mr. X em uma multidão de 150 pessoas: a pessoa que quer que ele chama alto o suficiente para que todos na sala pode ouvi-los, esperando que ele responderia se ele está lá. Quando ele responde, sabemos que a pessoa que ele é.

Quando ARP quer encontrar o endereço Ethernet correspondente a um determinado endereço IP, ele usa um recurso Ethernet chamada *radiodifusão*, Em que um datagrama é dirigido a todas as estações da rede simultaneamente. O amplo datagrama elenco enviadas por ARP contém uma consulta para o endereço IP. Cada host receptor compara essa consulta para a sua
próprio endereço IP e se ele corresponde, retorna uma resposta ARP para o host perguntando. O host perguntando agora pode extrair
o endereço do remetente Ethernet da resposta.

Você pode perguntar como um anfitrião pode chegar a um endereço de Internet que pode estar em um meio de rede diferentes ao

redor
o mundo. A resposta a esta pergunta envolve *roteamento*, Ou seja, encontrar a localização física de um host em uma rede-de trabalho. Vamos discutir esta questão na próxima seção.

Vamos falar um pouco mais sobre a ARP. Depois de uma série descobriu um endereço Ethernet, que armazena em seu cache

ARP
para que ele não tem que consultar novamente na próxima vez que quiser enviar um datagrama para o host em questão. No entanto, não é sensato manter essas informações sempre; placa do host remoto Ethernet pode ser substituído por de problemas técnicos, de modo a entrada ARP se torna inválida. Portanto, as entradas no cache ARP são descartados após algum tempo para forçar a outra consulta para o endereço IP.

Às vezes também é necessário encontrar o endereço IP associado com um endereço Ethernet fornecido. Isso acontece quando uma máquina sem disco rígido quer para arrancar a partir de um servidor na rede, que é uma situação comum no local Networks. Um cliente sem disco, no entanto, não tem praticamente nenhuma informação sobre si mesmo - com exceção de seu endereço Ethernet!
Então, ele transmite uma mensagem que contém um pedido solicitando um servidor de boot para fornecê-lo com um endereço IP. Não há
outro protocolo para esta situação chamado *Reverse Address Resolution Protocol* (RARP). Junto com o BOOTP protocolo, que serve para definir um procedimento de bootstrapping clientes sem disco na rede.

Roteamento IP

Vamos agora levantar a questão de encontrar o host que os datagramas ir com base no endereço IP. Diferentes partes do o endereço são tratadas de formas diferentes, é o seu trabalho para configurar os arquivos que indicam como tratar cada parte.

Redes IP

Quando você escreve uma carta para alguém, você costuma colocar o endereço completo no envelope indicando o país, Estado e CEP. Depois de colocá-lo na caixa de correio, os correios vão entregá-lo ao seu destino: ele será enviado para o país indicado, onde o serviço nacional despachá-lo para o bom estado e região. A vantagem
deste esquema hierárquico é óbvia: onde quer que você mandar a carta, o postmaster local sabe mais ou menos que sentido de transmitir a carta, mas o postmaster não importa o caminho que a carta vai viajar, uma vez que atinge o seu país de destino.

redes IP são estruturados de forma semelhante. Em toda a Internet consiste de uma série de redes adequadas, chamado *sistemas autónomos*. Cada sistema executa roteamento entre os seus Estados-anfitriões internamente de modo que a tarefa de de-da ministrar um datagrama é reduzido a encontrar um caminho para a rede do host de destino. Assim que o datagrama é

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

entregue ao *qualquer* host na rede particular, o tratamento posterior é feito exclusivamente pela própria rede.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Sub-redes

Esta estrutura é refletida através da divisão de endereços IP em uma parte de host e rede, tal como explicado

anteriormente. Por
padrão, a rede de destino é derivado da parte de rede do endereço IP. Assim, os hosts com IP idênticos
rede números devem ser encontrados dentro da mesma rede.[15]

Não faz sentido oferecer um esquema semelhante *dentro* da rede, também, uma vez que pode consistir de uma coleção de

centenas
de redes menores, com as menores unidades físicas como sendo redes Ethernet. Portanto, IP permite que você
subdividir uma rede IP em vários *sub-redes*.

Uma sub-assume a responsabilidade de entregar datagramas para um determinado intervalo de endereços IP. É uma extensão do
conceito de campos de bits de divisão, como nas classes A, B e C. No entanto, a parte de rede é agora alargado a in-
cluir alguns bits da parte de host. O número de bits que são interpretadas como o número de sub-rede é dada pela
chamada *máscara de sub*-Ou *netmask*. Este é um número de 32 bits também, que especifica a máscara de bits para a parte de
rede
do endereço IP.

A rede do campus da Universidade de Groucho Marx é um exemplo de uma rede deste tipo. Ele tem uma rede classe B
número de *149.76.0.0*, E sua máscara de rede é, portanto, *255.255.0.0*.

Internamente, a rede do campus GMU consiste de várias redes menores, como LANs vários departamentos ". Assim
o intervalo de endereços IP é dividido em 254 sub-redes, *149.76.1.0* através *149.76.254.0*. Por exemplo, o de-
partamento de Física Teórica, foi atribuído *149.76.12.0*. A espinha dorsal do campus é uma rede em sua própria
direito, e é dada *149.76.1.0*. Estes sub-dividir o mesmo número de rede IP, enquanto o terceiro octeto é usado para
distingui-las. Eles vão, portanto, usar uma máscara de sub- *255.255.255.0*.

Figura 2.1 shoFoi assim que *149.76.12.4*, O endereço do *quark*, É interpretada de forma diferente quando o endereço é tomado

como
uma rede de classe B comuns e quando usado com sub-redes.

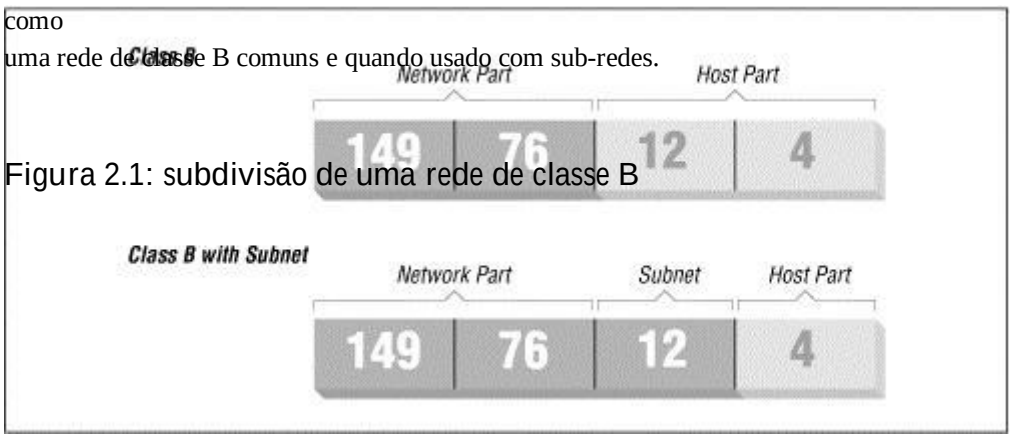


Figura 2.1: subdivisão de uma rede de classe B

É interessante notar que *subnetting* (A técnica de sub-geração) é apenas um *divisão interna* da-net
de trabalho. Sub-redes são gerados pelo proprietário da rede (ou os administradores). Freqüentemente, sub-redes são criadas para
reflectir as limitações existentes, sejam elas físicas (entre dois Ethernets), administrativa (entre dois departamentos),
ou geográfica (entre as duas localidades), e autoridade sobre cada sub-rede é delegada a uma pessoa de contato.
No entanto, essa estrutura afeta apenas o comportamento interno da rede, e é completamente invisível para o exterior
mundo.

Gateways

Sub-rede não é apenas um benefício para a organização, e é frequentemente uma consequência natural da bounda hardware
Rés. O ponto de vista de um host em uma determinada rede física, como uma rede Ethernet, é muito limitada: só pode

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

fale com o anfitrião da rede onde ele está. Todos os outros hosts podem ser acessados somente através de máquinas especiais

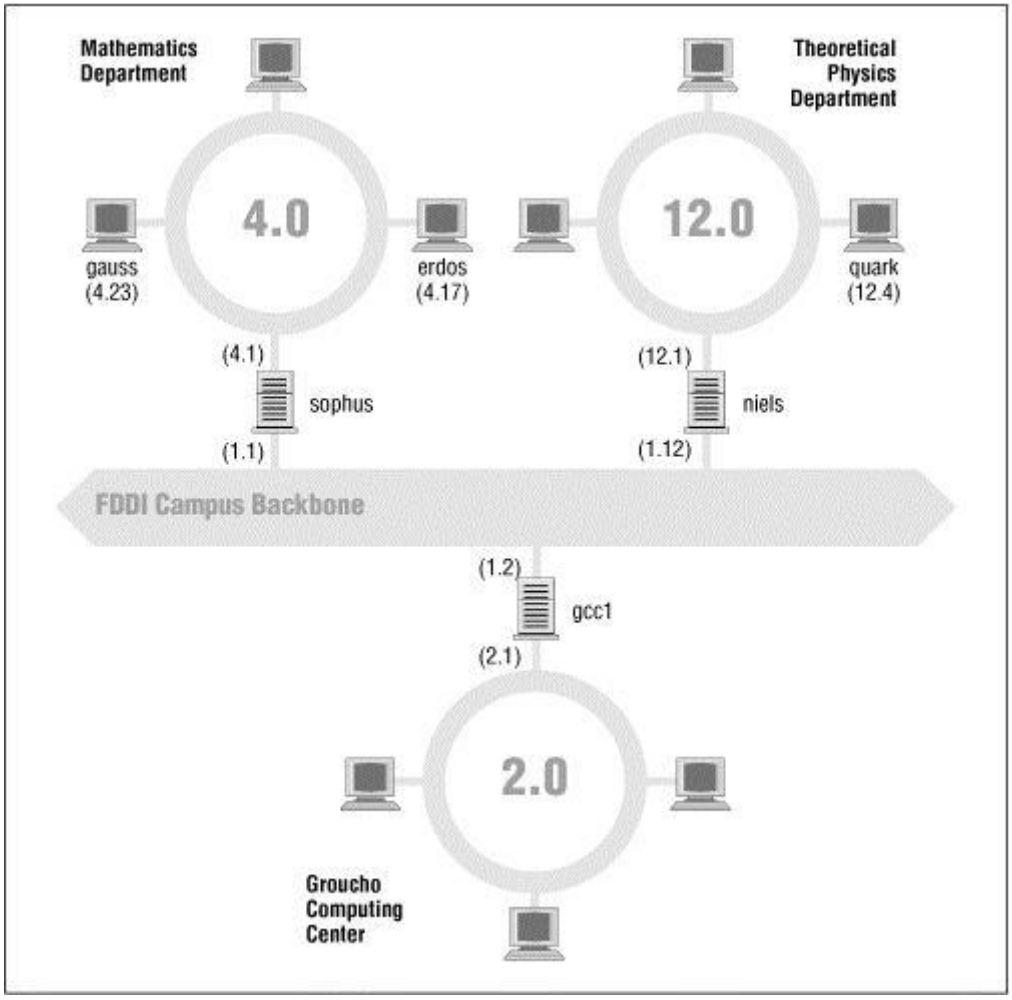
15 Os sistemas autônomos são um pouco mais geral. Podem incluir mais de uma rede IP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

chamada *gateways*. Um gateway é um host que está conectado a duas ou mais redes físicas e simultaneamente é configurado para comutar pacotes entre eles.

Figura 2.2 scomos parte da topologia de rede em Groucho Marx University (GMU). Hosts que estão em dois sub-redes ao mesmo tempo, são mostrados com os dois endereços.

Figura 2.2: Uma parte da topologia de rede em Groucho Marx Universidade



Redes físicas diferentes que pertencem a diferentes redes IP para IP para ser capaz de reconhecer se um host está em um rede local. Por exemplo, o número de rede *149.76.4.0* é reservada para os hosts da LAN matemática.
Ao enviar um datagrama para *quark*, O software de rede em *Erdos* vê imediatamente a partir do endereço IP *149.76.12.4* que o host de destino está em uma rede física diferente e, portanto, só pode ser alcançado através de um gateway (*sophus* por padrão).

sophus se estiver conectado a duas sub-redes distintas: o departamento de Matemática e do backbone do campus. É acessos de cada um através de uma interface diferente, *eth0* e *fddi0*, Respectivamente. Agora, o endereço IP podemos atribuí-la? Devemos dar-lhe um na sub-rede *149.76.1.0*, Ou em *149.76.4.0*?

A resposta é "ambos". *sophus* tem sido atribuído o endereço *149.76.1.1* para uso na *149.76.1.0* rede e endereço *149.76.4.1* para uso na *149.76.4.0* rede. Um gateway deve ser atribuído um endereço IP para cada rede, trabalho a que pertence. Esses endereços - juntamente com a máscara correspondente - estão ligados à interface através da que a sub-rede é acessada. Assim, o mapeamento da interface e endereço para *sophus* ficaria assim:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Interface	Endereço	Netmask
eth0	149.76.4.1	255.255.255.0
fddi0	149.76.1.1	255.255.255.0
eis	127.0.0.1	255.0.0.0

A última entrada descreve a interface loopback *eis*, Que falamos anteriormente.

Geralmente, você pode ignorar a sutil diferença entre a atribuição de um endereço de um host ou a sua interface. Para hosts que estão em uma única rede, como *Erdos*, Você geralmente se referem ao host como tendo esta e que o endereço IP, embora estritamente falando, é a interface Ethernet que tem este endereço IP. A distinção é muito importante somente quando se referir a um gateway.

A tabela de roteamento

Vamos agora concentrar a nossa atenção sobre como escolher um gateway IP para usar para entregar um datagrama para uma

rede remota.

Temos visto que *Erdos*, Quando recebe um datagrama para *quark*, Verifica o endereço de destino e descobre que não é na rede local. *Erdos* portanto, envia o datagrama para o gateway padrão *sophus*, Que está agora confrontado com a mesma tarefa. *sophus* reconhece que *quark* não é em qualquer uma das redes que está conectado diretamente, por isso tem que encontrar uma outra porta de entrada para encaminhá-lo completamente. A escolha correta seria *niels*, A porta de entrada para a Física
departamento. *sophus* portanto, necessita de informações para rede de associados de um destino com um gateway adequado.

IP utiliza uma tabela para essa tarefa que associa as redes com os gateways através do qual eles podem ser alcançados. Um

catch-
todas as entradas (o *rota padrão*) Geralmente deve ser fornecido também, este é o gateway da rede associada *0.0.0.0*. Todos os endereços de destino coincidir com esta rota, já que nenhum dos 32 bits são necessários para correspondência, e, portanto, os pacotes
a uma rede desconhecida são enviados através da rota padrão. Em *sophus*, A tabela pode ter este aspecto:

Rede	Netmask	Gateway	Interface
149.76.1.0	255.255.255.0	-	*fddi0*
149.76.2.0	255.255.255.0	149.76.1.2	*fddi0*
149.76.3.0	255.255.255.0	149.76.1.3	*fddi0*
149.76.4.0	255.255.255.0	-	*eth0*
149.76.5.0	255.255.255.0	149.76.1.5	*fddi0*
...	...	...	...
0.0.0.0	0.0.0.0	149.76.1.2	*fddi0*

Se você precisa usar uma rota para uma rede que *sophus* está diretamente conectado, você não precisa de um gateway, o porta-coluna para cá contém um hífen.

O processo para identificar se um determinado endereço de destino corresponde a uma rota é uma operação matemática. O processo é bastante simples, mas exige uma compreensão da lógica e aritmética binária: Uma rota corresponde a um destino, se o endereço de rede lógica AND com a máscara exatamente igual ao endereço de destino lógica AND com a máscara.

Tradução: um percurso partidas se o número de bits do endereço de rede especificado pela máscara (a partir de
o bit mais à esquerda, o bit de ordem mais elevada de um byte do endereço) corresponder o mesmo número de bits do destino

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

endereço.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Quando a execução IP está procurando a melhor rota para um destino, pode encontrar um número de roteamento entradas que corresponde ao endereço de destino. Por exemplo, sabemos que a rota padrão corresponde a cada destino, mas datagramas destinados a redes conectadas localmente irá corresponder a sua rota local, também. Como se sabe qual IP rota a ser utilizada? É aqui que a máscara de rede desempenha um papel importante. Embora ambas as rotas coincidir com o destino, um dos as rotas tem um maior do que a outra máscara. Nós mencionado anteriormente que a máscara foi utilizada para quebrar o nosso espaço de endereçamento em redes menores. Quanto maior a máscara, mais especificamente um endereço de destino é pareados, quando roteamento de pacotes, devemos sempre escolher a rota que tem a maior máscara de rede. O padrão rota tem uma máscara de bits zero, e na configuração apresentada acima, as redes conectadas localmente têm um 24 bits máscara. Se um datagrama corresponda a uma rede conectada localmente, ele será encaminhado para o dispositivo apropriado na
preferência para seguir a rota padrão, pois a rota de rede local coincide com um maior número de bits.
Os datagramas apenas que serão encaminhadas através da rota padrão são aqueles que não correspondem a qualquer outra rota.

Você pode criar tabelas de roteamento por uma variedade de meios. Para pequenas redes locais, é geralmente mais eficiente para

construí-los
à mão e alimentá-los para o IP usando o `rota` comando em tempo de boot (veja o capítulo 5, *Configurando o TCP Net / IP-trabalho*). Para redes maiores, eles são construídos e ajustados em tempo de execução *daemons de roteamento*; Estes daemons executado em
hosts central da rede e trocar informações de roteamento para calcular "ótimo" rotas entre o membro redes.

Dependendo do tamanho da rede, você vai precisar usar diferentes protocolos de roteamento. Para o roteamento dentro

Autônoma de
sistemas de autônomo (como o campus do Groucho Marx), a *protocolos de roteamento interno* são utilizados. O mais proeminente uma delas é a *Routing Information Protocol* (RIP), que é implementado pela BSD `roteado` daemon. Para roteamento entre sistemas autônomos, *protocolos de roteamento externos* como *Externas Gateway Protocol* (EGP) ou *Border Gateway Protocol* (BGP) devem ser utilizados, estes protocolos, incluindo RIP, têm sido implementadas no Universidade de Cornell `gated` daemon.

Metric Valores

Nós dependemos de roteamento dinâmico para escolher a melhor rota para um host de destino ou de rede com base no número

de
lúpulo. O lúpulo é um dos gateways datagrama tem de passar antes de chegar a um host ou rede. O menor é uma rota, a melhores taxas de RIP-lo. Muito rotas longas, com 16 ou mais lúpulo são considerados inutilizáveis e são descartados.

RIP gerencia informações de roteamento interno em sua rede local, mas você tem que correr `gated` em todos os hosts. Em tempo de inicialização, `gated` controlos para todas as interfaces de rede ativa. Se houver mais de uma interface ativa (não contagem
ção da interface de loopback), ele assume o anfitrião é comutação de pacotes entre diferentes redes e activamente trocar e difundir informações de roteamento. Caso contrário, será apenas passivamente receber atualizações RIP e atualização a tabela de roteamento local.

Quando as informações de difusão a partir da tabela de roteamento local, `gated` calcula o comprimento da rota a partir do chamada *valor métrico* associados com a entrada da tabela de roteamento. Este valor métrico é definido pela administração do sistema
tor ao configurar a rota, e deve reflectir os custos reais de rota.[16] Portanto, a métrica de uma rota para um sub-rede que o host está diretamente ligado ao deve ser sempre zero, enquanto que uma rota passando por dois gateways deve ter uma métrica de dois. Você não tem que se preocupar com a métrica, se você não usar `RIP` ou `gated`.

O Internet Control Message Protocol

IP tem um protocolo companheiro que nós não falamos sobre isso ainda. Este é o *Internet Control Message Protocol* (ICMP), usado pelo código do kernel de rede de comunicação de mensagens de erro para outros hospedeiros. Por exemplo, suponha ~~que estão no *Erdos* novamente e qu~~ero `telnet` para a porta 12345 no *quark*, Mas não há nenhum processo de escuta em que porto. Quando o primeiro pacote TCP para esta porta chega *quark*, A camada de rede irá reconhecer esta chegada e imediatamente retornar uma mensagem ICMP *Erdos* afirmando que "Port Unreachable".

O protocolo ICMP fornece várias mensagens diferentes, muitas das quais lidar com situações de erro. No entanto, ~~uma~~ uma mensagem menos interessante, chamado de mensagem de redirecionamento é gerado pelo módulo de roteamento

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

quando
detecta que outro host está usando-o como um gateway, apesar de um percurso muito mais curto existe. Por exemplo, após inicialização, a tabela de roteamento de *sophus* pode ser incompleta. Ela pode conter as rotas para a rede de Matemática, ao backbone FDDI, ea rota padrão apontando para o gateway Groucho Computing Center (gcc1). Assim,

16 O custo de uma rota pode ser pensado, em um caso simples, como o número de saltos necessários para alcançar o destino. Adequada de cálculo de custos rota pode ser uma arte em projetos de redes complexas.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

pacotes para *quark* seria enviado para *gcc1* ao invés de *niels,* A porta de entrada para o departamento de

Física. Quando re-
ceiving como um datagrama, *gcc1* notará que esta é uma má escolha de rota e encaminhará o pacote para *niels*, entretanto, retornando uma mensagem de redirecionamento ICMP para *sophus* contá-la da rota superior.

Esta parece ser uma maneira muito inteligente para evitar qualquer configuração manual, mas as rotas mais básicas. No entanto,

ser
advertiu que confiar em esquemas de roteamento dinâmico, seja RIP ou mensagens de redirecionamento ICMP, nem sempre é uma boa
idéia. ICMP Redirect e RIP oferecem pouca ou nenhuma escolha na verificação de que algumas informações de roteamento é de fato
autêntico. Esta situação permite maliciosos bom-para-nadas para interromper o tráfego da rede inteira, ou mesmo
pior. Conseqüentemente, o código de rede do Linux trata as mensagens de redirecionamento rede como se fossem Host Redi-
retângulos. Isso minimiza o dano de um ataque, restringindo-a apenas um host, ao invés de toda a rede. Em
Do outro lado, isso significa que um pouco mais o tráfego é gerado no caso de uma condição legítima, uma vez que cada host
faz com que a geração de uma mensagem de redirecionamento ICMP. É geralmente considerado má prática de invocar ICMP
redireciona para nada nestes dias.

Resolver nomes de host

Como descrito anteriormente, abordando em redes TCP / IP, pelo menos para IP versão 4, gira em torno de 32-bit
números. No entanto, você terá dificuldade de lembrar mais do que alguns destes números. Portanto, os anfitriões
são geralmente conhecidos por "normais" de nomes como *gauss* ou *estranho*. Torna-se obrigação do aplicativo para encontrar o
Endereço IP correspondente a este nome. Este processo é chamado *resolução de nomes*.

Quando um aplicativo precisa para localizar o endereço IP de um determinado host, ele conta com as funções da biblioteca

gethostby-
nome (3) e *gethostbyaddr (3)*. Tradicionalmente, estas e uma série de procedimentos relacionados foram agrupadas em uma sepa-
biblioteca chamada de taxa de *resolverlibrary*; No Linux, essas funções são parte do padrão *libc*. Popularmente, esta
coleção de funções é, portanto, referida como "a resolver." Resolver o nome de configuração está detalhado no Chap-
ter 6, *Nome do serviço e configuração Resolver*.

Em uma pequena rede como uma rede Ethernet ou mesmo um cluster de Ethernet, não é muito difícil manter as tabelas mapa
ping hostnames para endereços. Esta informação é normalmente mantida em um arquivo chamado */ Etc / hosts*. Ao adicionar ou remov-
ing hosts, ou reafectação de endereços, tudo que você tem a fazer é atualizar o *hosts* arquivo em todos os hosts. Obviamente, isso vai
tornar-se pesado com as redes que compõem a mais do que um punhado de máquinas.

Uma solução para este problema é a *Rede de Sistema de Informação* (NIS), desenvolvida pela Sun Microsystems, collo-
quially chamado YP ou Páginas Amarelas. armazena o NIS *hosts* imagem (e outras informações) em um banco de dados em um mestre
host a partir do qual os clientes podem recuperá-lo quando necessário. Ainda assim, esta abordagem é adequado apenas para redes de médio porte
como LAN, porque envolve a manutenção de todo o *hosts* banco de dados central e distribuí-lo para todos os servi-
ers. NIS instalação e configuração é discutido em detalhes no Capítulo 13, *O Sistema de Informação de Rede*.

Na internet, informações sobre o endereço foi inicialmente armazenado em um único *HOSTS.TXT* banco de dados, também. Este

arquivo foi
mantido no *Network Information Center* (NIC), e teve de ser baixado e instalado por todos os participantes
sites. Quando a rede cresceu, vários problemas surgiram com esse esquema. Além da sobrecarga administrativa
envolvidos na instalação *HOSTS.TXT* regularmente, a carga sobre os servidores que distribuiu tornou-se demasiado elevado. Mesmo
mais grave, todos os nomes tiveram de ser registrado com o NIC, que assegurou que nenhum nome foi publicado duas vezes.

Por isso, um esquema de resolução de novo nome foi adotado em 1994: o *Domain Name System*. O DNS foi concebido
por Paul Mockapetris e endereços de dois problemas simultaneamente. Discutimos o Domain Name System, em
detalhes no Capítulo 6.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 3 - Configurando o hardware de rede

Temos conversado bastante sobre as interfaces de rede geral e TCP / IP emite, mas nós realmente não abrangidos o que acontece quando o "código de rede" no kernel acessa uma peça de hardware. Para descrever essa precisamente, temos que falar um pouco sobre o conceito de interfaces e drivers.

Primeiro, é claro, há o próprio hardware, como por exemplo uma rede Ethernet, FDDI ou Token Ring cartão: esta é uma fatia de Epóxi desordenados com lotes de pequenos chips com números estranhos sobre eles, sentado em um slot do seu PC. Isto é o que que geralmente chamamos de um dispositivo físico.

Para você usar uma placa de rede, funções especiais têm de estar presentes em seu kernel Linux que compreendem a modo particular este dispositivo é acessado. O software que implementa estas funções é chamado de *driver de dispositivo*. O Linux tem drivers para muitos tipos diferentes de cartões de interface de rede: ISA, PCI, MCA, EISA, Paralela porto, PCMCIA, e, mais recentemente, USB.

Mas o que queremos dizer quando dizemos que um condutor "pegas" um dispositivo? Vamos considerar uma placa Ethernet. O motorista tem
ser capaz de comunicar com os periféricos de lógica no cartão de alguma forma: ele tem de enviar comandos e dados para o cartão, enquanto o cartão deve entregar os dados recebidos para o motorista.

Em estilo IBM computadores pessoais, a comunicação acontece através de um conjunto de endereços de I / O que são mapeados para registros no cartão e / ou através de transferências de memória compartilhada ou direta. Todos os comandos e os dados
kernel envia para o cartão tem que ir para esses endereços. E / S e endereços de memória são geralmente descritos por fornecendo o ponto de partida ou *endereço base*. endereços de base típica de placas Ethernet ISA de ônibus são `0x280` ou `0x300`.
placas de rede PCI bus geralmente têm suas endereço E / S automaticamente atribuído.

Normalmente você não precisa se preocupar com qualquer problema de hardware, como o endereço de base porque o kernel faz uma
tentativa de arranque para detectar a localização de um cartão. Isso é chamado *auto sondagem*, O que significa que o kernel lê memória de vários ou de I / O locais e compara os dados que ele lê lá com o que seria de esperar para ver se um certo placa de rede foram instalados no local. No entanto, pode haver placas de rede ele não consegue detectar automaticamente; isso às vezes é o caso de placas de rede que são baratos não muito clones de cartões padrão de outros fabri-fabricantes. Além disso, o kernel normalmente tenta detectar apenas um dispositivo de rede durante a inicialização. Se você estiver usando
mais de um cartão, você tem que dizer ao kernel sobre os outros cartões de forma explícita.

Outro parâmetro que poderá ter de dizer ao kernel é sobre a linha de solicitação de interrupção. componentes hardware ponentes geralmente interrompem o kernel quando eles precisam tomar cuidado - por exemplo, quando os dados chegaram ou um
condição especial ocorre. Em um PC barramento ISA, as interrupções podem ocorrer em um dos 15 canais de interrupção numeradas de 0, 1,
e 3 a 15. O número de interrupção atribuída a um componente de hardware é chamado de *número de pedido de interrupção* (IRQ).[17]

Conforme descrito no Capítulo 2, *Problemas de rede TCP / IP*, O kernel acessa um pedaço de hardware de rede através de um software chamado de construir uma *interface*. Interfaces oferecer um conjunto abstracto de funções que são os mesmos
em todos os tipos de hardware, como o envio ou recepção de um datagrama.

As interfaces são identificadas por meio de nomes. Em muitos outros sistemas operacionais Unix-like, a interface de rede é implementado como um arquivo de dispositivo especial na */ Dev /* diretório. Se você digitar o `ls-las / dev /` comando, você
vai ver o que esses arquivos de dispositivo semelhante. No permissões de arquivos (segunda) coluna, você verá que os arquivos do dispositivo
começar com uma letra em vez do hífen visto para arquivos normais. Este caractere indica o tipo de dispositivo. A a maioria dos tipos de dispositivos mais comuns são `b`, O que indica que o dispositivo é uma *bloco* dispositivo e manipula blocos inteiros de dados
com cada um ler e escrever, e `c`, O que indica que o dispositivo é uma *caráter* dispositivo e manipula os dados de um caracter ao mesmo tempo. Sempre que você normalmente vê o tamanho do arquivo na `ls` saída, você verá dois números ao invés, chamado
os maiores e menores números de dispositivo. Estes números indicam o dispositivo com o qual o arquivo de dispositivo é

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

associados.

Cada driver de dispositivo registra um número único grande com o kernel. Cada *instância* desse dispositivo registra um menor número único para esse dispositivo principal. A `tty` interfaces,*/ Dev / tty **, São um dispositivo de modo de caracteres indicada
pelo "`c`", E cada um tem um maior número de 4, Mas */ Dev/tty1* tem um número menor de `1`E */ Dev/tty2* tem um menor

17 IRQs 2 e 9 são os mesmos, porque o design de PCs da IBM tem dois processadores de interrupção em cascata, com oito IRQs cada; do secundário processador é ligado ao IRQ 2 do primário.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

número de 2. Arquivos de dispositivos são muito úteis para muitos tipos de dispositivos, mas pode ser

desajeitado para usar quando se tenta
encontrar um dispositivo não utilizado para abrir.

nomes de interface Linux são definidas internamente no kernel e não são arquivos de dispositivos no */ Dev*

diretório. Alguns
nomes de dispositivos são listados mais tarde, em "A Volta da Linux Network Devices". "A atribuição de interfaces para
dispositivos geralmente depende da ordem na qual os dispositivos são configurados. Por exemplo, a primeira placa Ethernet em
impasse será *eth0*, E os próximos serão *eth1*. interfaces SLIP são tratadas de maneira diferente dos outros porque eles são atribuídos dinamicamente. Sempre que uma conexão SLIP é estabelecida, uma interface é atribuído à série porto.

Figura 3.1 illudemonstra a relação entre o hardware, drivers de dispositivos e interfaces.

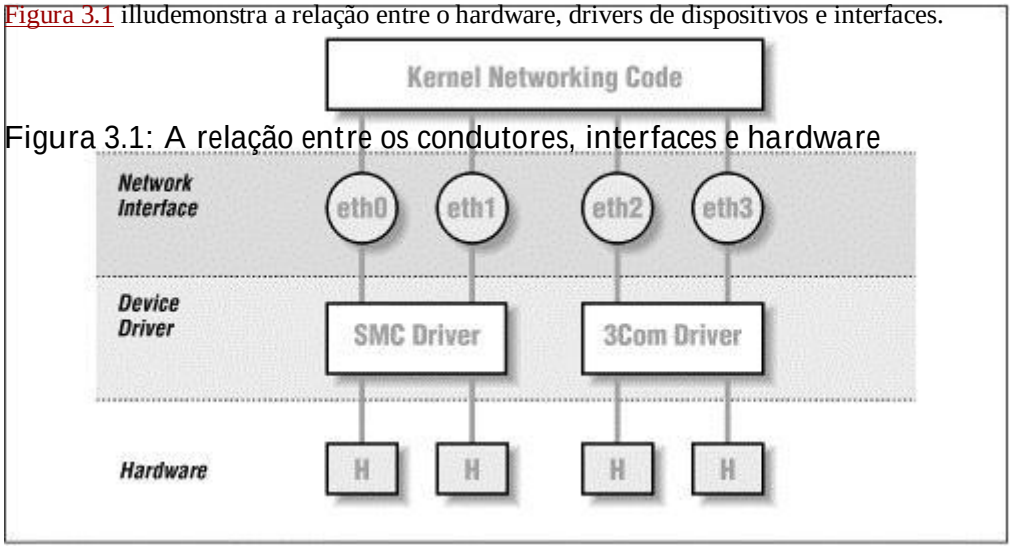


Figura 3.1: A relação entre os condutores, interfaces e hardware

Quando a inicialização, o kernel exibe os dispositivos ele detecta e as interfaces que ele instala. O seguinte é um excerto a partir de mensagens típicas de inicialização:

```
  .
  .  Este processador de honra o bit WP, mesmo quando em modo de supervisor /.
     Boas.
Sociedade de Computação da Universidade de Swansea NET3.035 para Linux 2.0
NET3: Unix domain sockets 0,13 para Linux NET3.035.
Universidade de Swansea TCP Sociedade de Computação / IP para NET3.034
Protocolos IP: IGMP, ICMP UDP, TCP
Universidade de Swansea IPX Computer Society 0,34 para NET3.035
IPX Copyright Partes (c) 1995 Caldera, Inc.
Versão do driver Serial 4,13 sem opções serial ativada
tty00 na 0x03f8 (irq = 4) é um 16550A
tty01 na 0x02f8 (irq = 3) é um 16550A
CSLIP: Código de copyright 1989 Reitoria da Universidade da Califórnia
PPP: Versão 2.2.0 (alocação dinâmica de canais)
PPP canal dinâmico de alocação de direitos autorais código 1995 Caldera, Inc.
PPP disciplina da linha registrado.
eth0: 3c509 em 0x300 tag 1, 10baseT porta, o endereço 00 a0 24 0e e4 e0 /
    IRQ 10.
3c509.c: 1,12 6/4/97 becker@cesdis.gsfc.nasa.gov
Linux versão 2.0.32 (root @ perf) (gcc versão 2.7.2.1)
# 01 de outubro Ter 21 15:30:44 EST 1997
  .
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

.

Este exemplo mostra que o kernel foi compilado com o TCP / IP habilitado, e inclui drivers para SLIP, CSLIP e PPP. A terceira linha do fundo, diz que uma placa Ethernet 3C509 foi detectado e instalado como interface *eth0*. Se você tem algum outro tipo de placa de rede - talvez um adaptador de bolso D-Link, por exemplo - geralmente o kernel irá imprimir uma linha que começa com seu nome de dispositivo - *dl0* no exemplo D-Link - seguido pelo tipo de cartão detectado. Se você tiver uma placa de rede instalado, mas não vejo qualquer mensagem semelhante, o kernel é incapaz para detectar o seu cartão corretamente. Esta situação será discutida mais adiante na seção de "detecção automática Ethernet".

Configuração do Kernel

A maioria das distribuições Linux são fornecidas com os discos de inicialização que o trabalho para todos os tipos comuns de hardware de PC. Generaliado, o kernel fornecido é altamente modular e inclui quase todos os driver possível. Esta é uma ótima idéia para discos de boot, mas não é provavelmente o que você quer para o uso a longo prazo. Não há muito sentido em ter os drivers CLUTtering o disco que você nunca vai usar. Por isso, geralmente você vai rolar o seu próprio kernel e incluem apenas os drivers que você realmente precisa ou quer, dessa forma você salva um pouco espaço em disco e reduzir o tempo necessário para commonte um novo kernel.

Em qualquer caso, ao executar um sistema Linux, você deve estar familiarizado com a construção de um kernel. Pense nisso como um direito de passagem, uma afirmação de uma coisa que faz o software livre como poderoso como é - você tem a fonte. É não é um caso de "eu tenho que compilar um kernel," ao contrário, é um caso de "Eu *pode* compilar um kernel. "Os fundamentos da compilção de um kernel Linux são explicados no livro de Matt galês, *Rodando Linux* (O'Reilly). Portanto, vamos discutir únicas opções de configuração que afetam a rede nesta seção.

Um ponto importante que não vale a pena repetir aqui é a maneira como o kernel versão numeração obras regime. Linux kernels são numerados no seguinte formato: `2.2.14`. O primeiro dígito indica o *principais* número da versão. Este dígito muda quando há mudanças grandes e significativas para o projeto do kernel. Por exemplo, o kernel modificado a partir de 1 para 2 grandes quando o kernel obtido apoio para outras máquinas do que as máquinas Intel. O segundo número é o *menores* número da versão. Em muitos aspectos, este número é o número mais importante de se olhar. O Linux comunidade de desenvolvimento adotou um padrão em que *mesmo* Números menores indicam versão *produção*Ou *estável*, Caroços e *estranho* Números menores indicam versão *desenvolvimento*Ou *instável*, O miolo. As amêndoas são estáveis o que você deve usar em uma máquina que é importante para você, como eles têm sido mais exaustivamente testado. O dekernels senvolvimento é o que você deve usar se você estiver interessado em experimentar as novas funcionalidades do Linux, mas eles podem ter problemas que ainda não foram encontrados e consertados. O terceiro número é simplesmente incretadas para cada lançamento de uma versão secundária.[18]

Ao executar `make menuconfig`, Você é apresentado com um menu baseado em texto que oferece listas de configuração perguntas, como se pretende emulação matemática kernel. Uma dessas consultas pergunta se você quer Suporte para TCP / IP networking. Você deve responder a isso com `y` para ter um kernel capaz de rede.

Opções do Kernel na versão 2.0 do Linux e do Ensino Superior

Após a seção de opção geral estiver concluída, a configuração vai continuar a perguntar se você deseja incluir suporte para várias características, tais como drivers SCSI ou placas de som. O prompt vai indicar quais são as opções disponíveis. Você pode pressionar? para obter uma descrição do que a opção é realmente oferecendo. Você sempre terá o opção de sim (y) para incluir o componente estaticamente no kernel, ou não (n) para excluir o componente comcompletamente. Você também verá a opção (m) o módulo para os componentes que podem ser compilado como um tempo de execução carregáveis módulo. Módulos precisam ser carregados antes que eles possam ser usados e são úteis para os condutores de componentes que você utilizar com frequência.

A lista posterior de questões tratam de redes de apoio. O conjunto de opções de configuração está em confluxo constante devido ao desenvolvimento contínuo. Uma lista típica de opções oferecidas pela maioria das versões do kernel em torno de 2,0 e 2,1 parecido com este:

```
*
* Suporte ao dispositivo de rede
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
*
O dispositivo de rede de apoio (CONFIG_NETDEVICES) [Y / n /?]
```

18 As pessoas devem usar kernels em desenvolvimento e relatar se forem encontrados, o que é uma coisa muito útil se você tem uma máquina que você pode usada como uma máquina de teste. Instruções sobre como reportar bugs estão detalhados na */ Usr / src / linux / RELATÓRIOS-BUGS* na fonte do kernel Linux.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Você deve responder a essa pergunta com `y` Se você quiser usar *qualquer* tipo de dispositivos de rede, sejam eles
Ethernet, SLIP, PPP, ou coisa parecida. Quando você responder a pergunta com `y`, Suporte para dispositivos tipo Ethernet é
ativado automaticamente. Você deve responder a perguntas adicionais, se você quer ativar o suporte para outros tipos de
drivers de rede:

```
PLIP (porta paralela) de apoio (CONFIG_PLIP) [N / y / m /?] Y
PPP (ponto-a-ponto) de apoio (CONFIG_PPP) [N / y / m /?] Y
*
compressores * PCC para a PPP só é construído em módulos.
*
SLIP (serial line) support (CONFIG_SLIP) [N / y / m /?] M
 cabeçalhos CSLIP comprimido (CONFIG_SLIP_COMPRESSED) [N / y /?] y (NOVO)
 Keepalive e linefill (CONFIG_SLIP_SMART) [N / y /?] Y (NOVO)
 Seis bits encapsulamento SLIP (CONFIG_SLIP_MODE_SLIP6) [N / y /?] Y
 (NOVO)
```

Estas questões dizem respeito a protocolos de link várias camadas que o Linux suporta. Ambas as PPP e SLIP permitem que você
transporte de datagramas IP através de linhas seriais. PPP é na verdade um conjunto de protocolos utilizados para enviar o tráfego de rede entre
linhas seriais. Alguns dos protocolos que formam PPP gerir a forma que você autenticar-se para o dial-in
servidor, enquanto outros gerir a forma como certos protocolos são realizadas através do link - PPP não se limita à execução
TCP / IP datagramas, que pode também levar outros protocolos como o IPX.

Se você responder `y` ou `m` para suporte ao SLIP, você será solicitado a responder às três perguntas que aparecem abaixo.
A opção de cabeçalho comprimido fornece suporte para CSLIP, uma técnica que comprime os cabeçalhos TCP / IP como
menos de três bytes. Note que esta opção do kernel não liga CSLIP automaticamente, limitando-se a
funções do kernel necessárias para isso. A `Keepalive e linefill` opção faz com que o suporte SLIP para peri-
dicamente gerar atividade na linha SLIP a evitar a sua queda de um temporizador de inatividade. A `Seis bits encapsulamento SLIP` opção permite a execução de deslizar sobre as linhas e circuitos que não são capazes de transmiti-
ting se todos os dados de 8 bits limpa. Isso é semelhante à técnica uuencoding ou binhex usado para enviar binário
arquivos por correio electrónico.

PLIP fornece uma maneira de enviar datagramas IP através de uma conexão de porta paralela. É usado principalmente para se comunicar
com PCs rodando DOS. Em hardware PC típico, PLIP pode ser mais rápido do que o PPP ou SLIP, mas requer muito
sobrecarga da CPU para executar, por isso, enquanto a taxa de transferência pode ser bom, outras tarefas na máquina pode ser lento.

As perguntas seguintes endereços de placas de rede de vários fornecedores. Quanto mais motoristas estão sendo desenvolvidos, que
são susceptíveis de ver as perguntas acrescentado a esta secção. Se você quiser construir um kernel você pode usar em uma série de di-
ent máquinas, ou se a sua máquina tem mais de um tipo de placa de rede instalado, você pode habilitar mais de
um motorista:

```
  .
  .
Ethernet (10 ou 100Mbit) (CONFIG_NET_ETHERNET) [Y / n /?]
placas 3COM (CONFIG_NET_VENDOR_3COM) [Y / n /?]
3c501 apoio (CONFIG_EL1) [N / y / m /?]
3c503 apoio (CONFIG_EL2) [N / y / m /?]
3c509/3c579 apoio (CONFIG_EL3) [Y / m / n /?]
3c590/3c900 série (592/595/597/900/905) "Vortex / Boomerang" support /
    (CONFIG_VORTEX) [N / y / m /?]
AMD lança e PCnet (AT1500 e NE2100) apoio (CONFIG_LANCE) [N / y /?]
AMD PCInet32 (VLB e PCI) de apoio (CONFIG_LANCE32) [N / y /?] (NOVO)
Western Digital cartões SMC (CONFIG_NET_VENDOR_SMC) [N / y /?]
```

PDF Creator PDF4Free v2.0 http://www.pdf4fre.com

```
WD80 * 3 apoio (CONFIG_WD80x3) [N / y / m /?] (NOVO)
SMC apoio Ultra (CONFIG_ULTRA) [N / y / m /?] (NOVO)
SMC apoio Ultra32 (CONFIG_ULTRA32) [N / y / m /?] (NOVO)
SMC 9194 de apoio (CONFIG_SMC9194) [N / y / m /?] (NOVO)
Outras placas ISA (CONFIG_NET_ISA) [N / y /?]
Cabletron apoio E21xx (CONFIG_E2100) [N / y / m /?] (NOVO)
DEPCA, DE10x, DE200, DE201, suporte, DE202 DE422 (CONFIG_DEPCA) [N / y / m /?] /
    (NOVO)
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
EtherWORKS 3 (DE203, DE204, DE205) apoio (CONFIG_EWRK3) [N / y / m /?] (NOVO)
EtherExpress 16 de apoio (CONFIG_EEXPRESS) [N / y / m /?] (NOVO)
HP PCLAN + (27252A e 27247B) apoio (CONFIG_HPLAN_PLUS) [N / y / m /?] (NOVO)
HP PCLAN (27245 e outras séries 27XXX) apoio (CONFIG_HPLAN) [N / y / m /?] /
    (NOVO)
HP 10/100VG PCLAN (ISA, EISA, PCI) de apoio (CONFIG_HP100) [N / y / m /?] (NOVO)
NE2000/NE1000 apoio (CONFIG_NE2000) [N / y / m /?] (NOVO)
apoio SK_G16 (CONFIG_SK_G16) [N / y /?] (NOVO)
EISA, VLB, PCI e em controladores de cartão (CONFIG_NET_EISA) [N / y /?]
Apricot Xen-II na placa ethernet (CONFIG_APRICOT) [N / y / m /?] (NOVO)
Intel EtherExpress / support 100B Pro (CONFIG_EEXPRESS_PRO100B) [N / y / m /?] /
    (NOVO)
DE425, DE434, DE435, DE450, suporte DE500 (CONFIG_DE4X5) [N / y / m /?] (NOVO)
DECchip Tulip (dc21x4x) suporte PCI (CONFIG_DEC_ELCP) [N / y / m /?] (NOVO)
Número Intl. RightSwitch SE-X de apoio (CONFIG_DGRS) [N / y / m /?] (NOVO)
Pocket e adaptadores portátil (CONFIG_NET_POCKET) [N / y /?]
bolso AT-LAN-TEC/RealTek adaptador de apoio (CONFIG_ATP) [N / y /?] (NOVO)
D-Link DE600 suporte adaptador de bolso (CONFIG_DE600) [N / y / m /?] (NOVO)
D-Link DE620 suporte adaptador de bolso (CONFIG_DE620) [N / y / m /?] (NOVO)
Token Ring driver de apoio (CONFIG_TR) [N / y /?]
IBM chipset Tropic suporte adaptador de base (CONFIG_IBMTR) [N / y / m /?] (NOVO)
driver FDDI apoio (CONFIG_FDDI) [N / y /?]
Digital defea e DEFPA suporte adaptador (CONFIG_DEFXX) [N / y /?] (NOVO)
apoio ARCnet (CONFIG_ARCNET) [N / y / m /?]
  arc0e Enable (ARCnet "Éter-Encap" formato de pacote) (CONFIG_ARCNET_ETH) /
      [N / y /?] (NOVO)
  arc0s Enable (ARCnet formato de pacote RFC1051) (CONFIG_ARCNET_1051) /
      [N / y /?] (NOVO)
 .
 .
```

Finalmente, na seção de sistema de arquivos, o script de configuração irá perguntar se você quer suporte para NFS, o rede do sistema de arquivos. NFS permite exportar sistemas de arquivos de diversas máquinas, o que torna os arquivos aparecem como se estavam em um disco rígido comum ligado à máquina:

```
NFS suporte ao sistema de arquivos (CONFIG_NFS_FS) [y]
```

Nós descrevemos NFS em detalhes no Capítulo 14, *O Network File System*.

Opções de Rede no Kernel Linux 2.0.0 e do Ensino Superior

Linux 2.0.0 marcou uma mudança significativa em Redes Linux. Muitos recursos foram feitos um componente padrão do Kernel, como suporte para IPX. Um número de opções também foram adicionados e fez configurável. Muitas destas opções são usadas apenas em circunstâncias muito especiais e não vamos cobri-los em detalhe. O Networking HOWTO provavelmente endereços que não é coberto aqui. Vamos listar uma série de opções úteis nesta seção e explique quando você quer usar cada um deles:

Fundamentos

Para usar a rede TCP / IP, você deve responder a essa pergunta com y. Se você responder com nNo entanto, você ainda será capaz de compilar o kernel com suporte a IPX:

```
Networking options  --->
[*] Rede TCP / IP
```

Gateways

Você tem que ativar essa opção se o seu sistema atua como um gateway entre duas redes ou entre um LAN e uma ligação SLIP, etc Não faz mal para permitir isto por padrão, mas você pode desativá-lo para con- uma figura de acolhimento, como um chamado *firewall*. Firewalls são hosts que estão conectados a duas ou mais redes, mas não rotear o tráfego entre elas. Eles são comumente usados para fornecer aos usuários acesso à Internet em mini- risco normal para a rede interna. Os usuários são autorizados a fazer login no firewall e utilização de serviços de Internet, mas máquinas da empresa estão protegidos contra ataques externos, pois as conexões de entrada não pode cruzar o firewall (firewalls são abordados em detalhe no Capítulo 9, *Firewall TCP / IP*):

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
[*] IP: encaminhamento / gatewaying
```

Virtual Hosting

Essas opções, juntos, permitem a você configurar mais de um endereço IP em uma interface. Isto é algumvezes útil se você quiser fazer "virtual hosting", através do qual uma única máquina pode ser configurado para olhar e agir como se fosse realmente muitas máquinas separadas, cada uma com sua personalidade própria rede. Falaremos mais sobre IP aliasing em um momento:

```
[*] Network aliasing
<*> IP: apoio aliasing
```

Contabilidade

Esta opção permite-lhe recolher dados sobre o volume de tráfego IP que saem e chegam na sua máquina (Cobrimos isso é detalhe no Capítulo 10, *IP Contabilidade*):

```
[*] IP: contabilidade
```

abraço PC

Esta opção funciona em torno de uma incompatibilidade com algumas versões do PC / TCP, um comercial TCP / IP implementação para PCs baseados em DOS. Se você habilitar essa opção, você ainda será capaz de se comunicar com máquinas Unix normal, mas o desempenho pode ser prejudicado em ligações lentas:

```
--- (É seguro deixá-los intocados)
[*] IP: PC / TCP modo de compatibilidade
```

Diskless boot

Esta função permite *Reverse Address Resolution Protocol* (RARP). RARP é usado por clientes diskless e terminais X para solicitar o seu endereço IP durante a inicialização. Você deve habilitar RARP, se você pretende servir
este tipo de cliente. Um pequeno programa chamado `rarp`, Incluído com os utilitários de rede padrão, é usado adicionar entradas para a tabela RARP do kernel:

```
<*> IP: ARP reverso
```

MTU

Ao enviar dados sobre TCP, o kernel tem que quebrar a corrente em blocos de dados para passar para o IP. O tamanho do bloco é chamado de *Unidade Máxima de Transmissão*, Ou MTU. Para hosts que pode ser alcançado através de uma rede local, como uma rede Ethernet, é comum usar uma MTU tão grande quanto o comprimento máximo de
um pacote de Ethernet - 1.500 bytes. Quando roteamento IP sobre uma vasta área de rede como a Internet, é preferível utilizar datagramas de tamanho menor para garantir que eles não precisam de ser mais discriminados ao longo
o percurso através de um processo chamado *fragmentação IP*.[19] O kernel é capaz de determinar automaticamente o menor MTU de uma rota IP e configurar automaticamente uma conexão TCP para utilizá-lo. Esse comportamento é ativado por padrão. Se você responder `y` para esta opção esse recurso será desativado.

Se você quiser usar tamanhos menores do pacote de dados enviado para máquinas específicas (porque, por exemplo, os dados
passa por uma ligação SLIP), você pode fazer isso usando o `mss` opção do `rota` comando, que é brevemente discutido no final do presente capítulo:

```
[] IP: Path MTU Discovery Disable (normalmente ativado)
```

recursos de segurança

O protocolo IP suporta um recurso chamado *Source Routing*. Roteamento de origem permite que você especifique o percurso
um datagrama deve seguir pela codificação na rota para o datagrama em si. Esta era uma vez provavelmente útil antes de protocolos de roteamento como RIP e OSPF se tornou banal. Mas hoje é considerado um segurança ameaça, pois pode fornecer atacantes inteligente, com uma forma de contornar certos tipos de firewall proteção, ignorando a tabela de roteamento de um roteador. Você normalmente quer filtrar fonte datagramas encaminhados, por isso essa opção é normalmente habilitada:

```
[*] IP: Gota a rota de origem frames
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

19 Lembre-se que o protocolo IP pode ser realizada ao longo de muitos tipos diferentes de rede, e nem todos os tipos de rede irá suportar tamanhos de pacotes como
grande como Ethernet.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

suporte da Novell

Esta opção permite o suporte para IPX, o protocolo de transporte de rede Novell usa. Linux vai funcionar completamente feliz como um roteador IPX e este apoio é útil em ambientes onde você tem de arquivo Novell servidores. O sistema de arquivos NCP também requer suporte IPX habilitado em seu kernel, se você deseja anexar à e montar o seu sistema de arquivos Novell você deve ter esta opção habilitada (vamos dicuss IPX e os PCN sistema de arquivos no Capítulo 15, *IPX eo sistema de arquivos NCP*):

```
<*> O protocolo IPX
```

Radioamadorismo

Estas três opções de suporte para selecionar os três protocolos de Radioamador suportados pelo Linux: AX.25, NetRom e Rose (não descrevê-los neste livro, mas eles são abordados em detalhe no AX25 HOWTO):

```
<*> Amateur Radio AX.25 Level 2
<*> NET Rádio Amador / ROM
<*> Rádio Amador X.25 PLP (Rosa)
```

O Linux suporta outro tipo de driver: o motorista do manequim. A questão seguinte é exibida para o início da seção de driver de dispositivo:

```
<*> Dummy suporte de driver net
```

O motorista do manequim não fazer muito, mas é bastante útil em autônomo ou hospeda PPP / SLIP. É basicamente uma interface loopback mascarados. Em hosts que oferecem PPP / SLIP, mas não tenho outra rede em terface, você quer ter uma interface que suporta o seu endereço IP o tempo todo. Isto é discutido em um pouco mais detalhes em "A interface dummy" no Capítulo 5, *Configurando Redes TCP / IP*. Note-se que hoje você pode conseguir o mesmo resultado usando o recurso de alias IP e configurar o endereço IP como um alias na interface loopback.

Uma excursão de dispositivos de rede Linux

O kernel do Linux suporta um número de drivers de hardware para vários tipos de equipamento. Esta seção dá uma breve resumo das famílias de controladores estão disponíveis e os nomes de interface que eles usam.

Há uma série de nomes padrão para as interfaces do Linux, que estão listadas aqui. A maioria dos motoristas mais apoio de uma interface, caso em que as interfaces são numeradas, como em *eth0* e *eth1*:

eis

Esta é a interface loopback local. Ele é usado para fins de teste, bem como um par de rede aplicações. Ele funciona como um circuito fechado em que qualquer datagrama escrito para ele será imediatamente retornado para a camada de rede do host. Há sempre um dispositivo de loopback presente no kernel, e há pouco sentido em ter mais.

eth0,eth1, ...

Estas são as interfaces de placa Ethernet. Eles são usados para a maioria das placas Ethernet, incluindo muitos dos placas Ethernet de porta paralela.

tr0,tr1, ...

Estas são as interfaces de cartão Token Ring. Eles são usados para a maioria das placas Token Ring, incluindo os não-IBM
cartões manufaturados.

sl0,sl1, ...

Estas são as interfaces SLIP. interfaces SLIP são associados às linhas de série na ordem em que eles são alocados para SLIP.

ppp0,ppp1, ...

Estas são as interfaces PPP. Assim como interfaces SLIP, uma interface PPP está associado a uma linha serial uma vez que é convertido para o modo de PPP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

plip0,plip1, ...

Estes são os interfaces PLIP. PLIP transporta datagramas IP através de linhas paralelas. As interfaces são atri-
cados pelo condutor PLIP durante a inicialização do sistema e são mapeadas em portas paralelas. Na *2.0.x* kernels
há uma relação direta entre o nome do dispositivo e do porto de I / O da porta paralela, mas mais tarde
kernels os nomes dos dispositivos são alocados sequencialmente, assim como para dispositivos SLIP e PPP.

ax0,AX1, ...

Estas são as interfaces AX.25. AX.25 é o principal protocolo utilizado por operadores de rádio amador. AX.25
interfaces estão alocados e mapeados de forma similar aos dispositivos SLIP.

Existem muitos outros tipos de interfaces disponíveis para outros drivers de rede. Nós listamos apenas os mais comuns
queridos.

Durante as próximas seções, vamos discutir os detalhes de como usar os drivers descrito anteriormente. A Rede-
ing HOWTO fornece detalhes sobre como configurar a maioria dos outros, e os AX25 guia explica como
configurar os dispositivos de rede de rádio amador.

Instalação Ethernet

O código atual rede Linux suporta uma grande variedade de placas de rede. A maioria dos motoristas foram escritos por Donald
Becker, autor de uma família de drivers para placas baseadas no chip National Semiconductor 8390, estes têm
tornou conhecido como a Série Becker Drivers. Muitos outros desenvolvedores contribuíram drivers, e hoje há
são poucas placas Ethernet comuns que não são suportados pelo Linux. A lista de placas Ethernet suportados está crescendo
o tempo todo, por isso, se o seu cartão não é suportado ainda, as chances são de que será em breve.

Algum tempo mais cedo na história do Linux, teríamos tentado lista de todas as placas Ethernet com suporte, mas que
agora levar muito tempo e espaço. Felizmente, Paul Gortmaker mantém o HOWTO Ethernet, o que listas
cada uma das placas suportadas e fornece informações úteis sobre a obtenção de cada um deles rodando em Linux.[20] É
é enviada mensalmente ao comp.os.linux.answers newsgroup, e também está disponível em qualquer um dos Documentação
Linux
ção sites espelho do projeto.

Mesmo se você estiver confiante de que você sabe como instalar um determinado tipo de placa de rede em sua máquina, é

frequentemente
vale a pena dar uma olhada no que o HOWTO Ethernet tem a dizer sobre isso. Poderá encontrar mais informações que o ex-
tende para além das questões de configuração simples. Por exemplo, poderia poupar-lhe muitas dores de cabeça para saber o
comporta-
ior de algumas placas Ethernet DMA-base que utilizam o canal de DMA mesmo que o controlador SCSI Adaptec 1542 por
padrão. A menos que você mova uma delas para um canal DMA diferente, você vai acabar com a placa Ethernet
escrita de dados em pacotes em locais arbitrários no seu disco rígido.

Para usar qualquer uma das placas Ethernet suportada com o Linux, você pode usar um kernel pré-compilado a partir de um dos

principais
distribuições Linux. Estes geralmente possuem módulos disponíveis para todos os drivers de suporte, ea instalação
processo geralmente permite que você selecione quais os drivers que você pretende carregar. No longo prazo, no entanto, é melhor construir
o seu próprio kernel e compilar somente os drivers que você realmente precisa, o que economiza espaço em disco e memória.

Detecção automática Ethernet

Muitos dos drivers de Ethernet do Linux são inteligentes o suficiente para saber como procurar o local da sua Ethernet
cartão. Isto economiza ter de dizer ao kernel, onde é manualmente. As listas Ethernet HOWTO se um espe-
driver lar usa detecção automática e em qual ordem ele procura o endereço de I / O para o cartão.

Há três limitações para o código de detecção automática. Primeiro, ele pode não reconhecer todos os cartões corretamente. Esta é

a espe-
especialmente verdadeiro para alguns dos clones mais baratos de cartas comuns. Em segundo lugar, o kernel não autoverificação
por mais de
uma carta a menos que especificamente instruído. Esta foi uma decisão de design consciente, como supõe-se que você vai querer
tem controle sobre a placa que é atribuído para cada interface. A melhor maneira de fazer isso de forma confiável é manualmente
con-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

a figura placas Ethernet em sua máquina. Em terceiro lugar, o motorista não pode sondar no endereço que o cartão é configurado para. De modo geral, os pilotos irão autoverificação para os endereços que a determinado dispositivo é capaz de sendo configurado, mas às vezes alguns endereços são ignorados, para evitar conflitos de hardware com outros tipos de cartões que normalmente utilizam esse mesmo endereço.

[20] Paulo pode ser alcançado em gpg109@rsphy1.anu.edu.au.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

placas de rede PCI deve ser detectados. Mas se você estiver usando mais de um cartão, ou se a autoverificação deve deixar de detectar o seu cartão, você tem uma maneira de dizer explicitamente que o kernel sobre o endereço da placa de base e nome.

Em tempo de boot, você pode fornecer argumentos e informações para o kernel que qualquer um dos componentes do kernel pode ler. Este mecanismo permite-lhe passar informações para o kernel que drivers Ethernet podem ser usados para localizar o seu hardware Ethernet sem fazer o teste driver.

Se você utilizar o lilo para inicializar o sistema, você pode passar parâmetros para o kernel, especificando-los através da *anexar* opção no *lilo.conf* arquivo. Para informar o kernel sobre um dispositivo Ethernet, você pode passar os seguintes parâmetros:

```
ether =irq,BASE_ADDR[param1, []param2,]nome
```

Os primeiros quatro parâmetros são numéricos, enquanto o último é o nome do dispositivo. A *irq*,*BASE_ADDR*E *nome* parâtros são necessários, mas os dois *param* parâmetros são opcionais. Qualquer um dos valores numéricos pode ser definido como zero, que faz com que o kernel para determinar o valor de sondagem.

O primeiro parâmetro define o IRQ atribuído ao dispositivo. Por padrão, o kernel tentará detectar automaticamente o dispositivo da IRQ canal. O driver 3c503, por exemplo, tem uma característica especial que seleciona um IRQ livre na lista de 5, 9, 3, 4 e configura o cartão para usar esta linha. A *BASE_ADDR* parâmetro fornece o endereço de E / S de base do cartão, valor de zero diz ao kernel para investigar os endereços listados acima.

drivers diferentes usam os próximos dois parâmetros de forma diferente. Para os cartões de memória compartilhada, como o WD80x3, eles especificar os endereços de início e término da área de memória compartilhada. Outras placas comumente usam *param1* para definir o nível no qual as informações de depuração é exibida. Valores de 1 a 7 denotam o aumento dos níveis de detalhamento, enquanto 8 desliga-os totalmente; 0 denota o padrão. O driver 3c503 usa *param2* a escolher entre o transceptor interno (padrão) ou um transceptor externo (um valor de 1). O primeiro utiliza o conector da placa BNC; este último utiliza o seu porta AUI. A *param* argumentos não devem ser incluídos em todos, se você não tem nada de especial configurar.

O primeiro argumento não numérico é interpretado pelo kernel como o nome do dispositivo. Você deve especificar um nome de dispositivo para cada placa de rede que você descreve.

Se você tiver duas placas de rede Ethernet, você pode ter Linux autodetect um cartão e passar os parâmetros da segunda carta de com `lilo`, Mas você provavelmente vai querer configurar manualmente duas placas. Se você decidir ter o teste do kernel para uma e configurar manualmente o segundo, você deve se certificar que o kernel não acidentalmente encontrar o segundo cartão em primeiro lugar, ou então o outro não será registrada em tudo. Você faz isso passando `lilo` um *reserva* opção, que explicitaretamente diz ao kernel para evitar sondagem do espaço de I / O tomadas pelo segundo cartão. Por exemplo, para tornar o Linux instalar uma segunda placa Ethernet na `0x300` como *eth1*, Você deve passar os seguintes parâmetros para o kernel:

```
Reserva = 0x300, 32 ether = 0,0 x300, eth1
```

A *reserva* opção garante que nenhum motorista acessa o segundo cartão é o espaço de I / O, quando a detecção de algum dispositivo.
Você também pode usar os parâmetros do kernel para substituir detecção automática de *eth0*:

```
Reserva = 0x340, 32 ether = 0,0 X340, eth0
```

Você pode desativar a detecção automática completamente. Você pode fazer isso, por exemplo, para parar um kernel de sondagem para uma rede Ethernet cartão que você poderia ter retirado temporariamente. Desativar detecção automática é tão simples como a especificação de um *BASE_ADDR* argumento de -1:

```
ether = 0, -1, eth0
```

Para fornecer esses parâmetros para o kernel em tempo de inicialização, você digita os parâmetros no lilo "boot:". Para ter `lilo` dar-lhe o "boot:" no prompt, você deve pressionar qualquer um dos, Control Alt ou Shift enquanto `lilo` está inicializando. Se você pressionar a tecla Tab no prompt, você será presenteado com uma lista de kernels que você

PDF Creator - PDF 4Free v2.0 http://www.pdf4free.com

pode inicializar. Para iniciar um kernel com os parâmetros fornecidos, digite o nome do kernel que você deseja inicializar, seguido por
um espaço, em seguida, os parâmetros que pretendem fornecer. Quando você pressiona a tecla Enter, `lilo` que irá carregar kernel e carregá-lo com os parâmetros que você fornecer.

Para fazer essa mudança ocorrer automaticamente a cada inicialização, digite os parâmetros para a */ Etc / lilo.conf* usando o `append =` palavra-chave. Um exemplo pode parecer como este:

```
boot = / dev / hda
root = / dev/hda2
install = / boot / boot.b
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
map = / boot / map
vga = normal
delay = 20
append = "ether = 10.300, eth0"

image = / boot/vmlinuz-2.2.14
label = 2.2.14
read-only
```

Depois de ter editado *lilo.conf*, Você deve executar novamente o `lilo` comando para ativar a mudança.

O Driver PLIP

IP em Linha Paralela (PLIP) é uma maneira barata de rede quando você deseja se conectar apenas duas máquinas. Ele usa um

Paral-
lel porta e um cabo especial, alcançando velocidades de 10 kilobytes por segundo para 20 kilobytes por segundo.

PLIP foi originalmente desenvolvido pela Crynwr, Inc. O seu design na época era genial (ou, se preferir, um hack), porque as portas paralelas original em PCs da IBM foram projetados para gastar seu tempo sendo unidirecional portas de impressora, as oito linhas de dados só podiam ser utilizadas para enviar os dados do PC para o dispositivo periférico, mas não o
contrário.[21] O projeto Cyrnwr PLIP contornado essa limitação, usando a porta de cinco linhas de status para a entrada, o que limitou a transferência de todos os dados como petiscos (bytes meia), mas também permitiu bidirecional trans-
fer. Este modo de operação foi chamada PLIP "modo 0." Hoje, as portas paralelas fornecido em hardware PC atender a completa transferência de dados bidirecional de 8 bits, e PLIP foi estendido para acomodar esta com a adição de PLIP "Modo 1".

Linux kernels até e incluindo a versão 2.0 dá suporte ao modo PLIP 0 apenas, e um controlador de porta paralela avançada existe como um patch para o kernel 2.0 e como uma parte padrão do código do kernel 2.2 para fornecer um modo de PLIP operação, também.[22] Diferentemente das versões anteriores do código PLIP, o motorista tenta agora ser compatível com o PLIP implementações de Crynwr, bem como o motorista PLIP no NCSA `telnet`.[23] Para conectar duas máquinas usando PLIP, você precisa de um cabo especial vendido em algumas lojas como uma impressora nulo ou cabo Laplink Turbo. Você pode, como-
nunca, fazer um você mesmo facilmente; Apêndice B, *Cabo configurações úteis* mostra como você.

O motorista PLIP para Linux é o trabalho de pessoas quase incontáveis. É atualmente mantido por Niibe Yutaka.[24]
Se compilado no kernel, o que configura uma interface de rede para cada uma das portas de impressão possível, com *plip0* corres-
correspondente à porta paralela *lp0*,*plip1* correspondente a *lp1*, Etc O mapeamento das interfaces para os portos difere nos 2,0 grãos e os kernels 2.2. Nos kernels 2.0, o mapeamento foi hardwired no *drivers / net / Spacd.c* arquivo na fonte do kernel. Os mapeamentos padrão nesse arquivo são:

Interface	Porta de I / O	IRQ
plip0	`0x3BC`	7
plip1	`0x378`	7
plip2	`0x278`	5

Se você configurou a porta de impressora de uma maneira diferente, você deve alterar esses valores em *drivers / net / Space.c* na Fonte do kernel Linux e construir um novo kernel.

No kernel 2.2, o motorista usa o PLIP "parport" driver compartilhamento de porta paralela desenvolvida por Philip Blundell.[25]
O novo driver aloca o PLIP nomes de dispositivo de rede de série, assim como para os motoristas Ethernet ou PPP, de modo que o

21 Lutar para limpar o nome de "hacking"! Sempre use "cracker" quando você está se referindo às pessoas que estão tentando conscientemente quebrar a segurança
de um sistema, e "hacker" quando você está se referindo a pessoas que encontraram uma maneira inteligente de resolver um problema. Hackers podem ser crackers.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

mas os dois nunca devem ser confundidas. Consulte o New Hackers Dictionary (popularmente encontrado no arquivo do jargão) para uma mais completa un-
tendimento dos termos.

22 O patch adaptador de porta paralela para melhorado kernel 2.0 está disponível http://www.cyberelk.demon.co.uk/parport.html.

23 NCSA `telnet` é um popular programa para DOS que executa o protocolo TCP / IP sobre Ethernet ou PLIP, e apoia `telnet` e FTP.

24 Niibe pode ser alcançado em gniibe@mri.co.jp.

25 Pode chegar a Philip *Philip.Blundell pobox.com* @.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

PLIP dispositivo criado pela primeira vez é *plip0*, O segundo é *plip1*E assim por diante. O hardware da porta paralela física é também atri-
cados em série. Por padrão, o driver de porta paralela tentará detectar o hardware de porta paralela com uma auto-
rotina da sonda, gravando as informações do dispositivo físico na ordem encontrada. É melhor prática para dizer explicitamente o kernel que eu físico / parâmetros S. Você pode fazer isso, fornecendo argumentos para o *parport_pc.o* módulo como carregá-lo, ou se você compilou o driver no kernel, usando o lilo para fornecer argumentos para o kernel no tempo de inicialização. A configuração de IRQ de qualquer dispositivo pode ser alterada posteriormente por escrito o valor novo para o IRQ relacionados
*/ Parport / proc / * / irq* arquivo.

Configurando o eu físico / parâmetros S em um kernel 2.2 ao carregar o módulo é simples. Para in-
postura, para dizer ao motorista que você tem duas PC-style portas paralelas em endereços de I / O `0x278` e `0c378` e IRQs 5 e 7, respectivamente, você deve carregar o módulo com os seguintes argumentos:

```
io modprobe parport_pc = 0x278, 0x378 irq = 5,7
```

Os argumentos correspondentes a passar para o kernel compilado para um motorista em são:

```
parport = 0x278, 5 parport = 0x378, 7
```

Você usaria o lilo *anexar* palavra-chave para que esses argumentos passados para o kernel na inicialização.

Quando o motorista PLIP é inicializado, quer em tempo de boot, se for embutida, ou quando o *plip.o* módulo é carregado, cada das portas paralelas terá um *plip* dispositivo de rede associado com ele. *plip0* será atribuído ao primeiro paralelo porta do dispositivo, *plip1* o segundo, e assim por diante. Você pode substituir manualmente esta atribuição automática usando outro conjunto
dos argumentos do kernel. Por exemplo, para atribuir `parport0` a dispositivo de rede `plip0`E `parport1` à rede dispositivo `plip1`, Você poderia usar os argumentos do kernel:

```
plip = parport1 plip = parport0
```

Este mapeamento não significa, porém, que você não pode usar essas portas paralelas para impressão ou outros fins.
Os dispositivos físicos de porta paralela são utilizadas pelo condutor PLIP apenas quando a interface correspondente é config-
figurado *até*.

Os drivers PPP e SLIP

Point-to-Point Protocol (PPP) e Serial Line IP (SLIP) são amplamente utilizados protocolos para o transporte de pacotes IP através de um
ligação em série. Um certo número de instituições oferecem PPP e SLIP acesso às máquinas que estão na Internet, assim fornecimento de conectividade IP a particulares (algo que de outra forma dificilmente acessíveis).

Nenhuma modificação de hardware são necessários para executar o PPP ou SLIP, você pode usar qualquer porta serial. Uma vez que con-porta serial
figuração não é específico para redes TCP / IP, temos dedicado um capítulo em separado para isso. Consulte o Chap-
No capítulo 4, *Configurando o Hardware Serial*, Para mais informações. Cobrimos PPP em detalhes no Capítulo 8, *O ponto-Protocolo a-Ponto*E SLIP no Capítulo 7, *Serial Line IP*.

Outros tipos de rede

A maioria dos outros tipos de rede estão configurados de forma semelhante ao Ethernet. Os argumentos passados para os módulos carregáveis
será diferente e alguns motoristas não podem suportar mais do que um cartão, mas quase tudo é o mesmo. Documentação para estes cartões é geralmente disponíveis no */ Usr / src / linux / Documentation / networking /* diretório do fonte do kernel Linux.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 4 - Configurando o Hardware Serial

A Internet está a crescer a um ritmo incrível. Grande parte deste crescimento é atribuído aos utilizadores da Internet que não

podem pagar
de alta velocidade à rede permanente e que usam protocolos como o SLIP, PPP, ou UUCP para discar para um provedor de rede para obter sua dose diária de e-mail e notícias.

Este capítulo é destinado a ajudar todas as pessoas que dependem de modems para manter a sua ligação com o mundo exterior.

Nós
não cobre a mecânica de como configurar o modem (o manual que veio com ele irá dizer-lhe mais sobre ele do que nós podemos), mas vamos cobrir a maior parte dos aspectos Linux específicas de gerenciamento de dispositivos que usam o serial
portos. Os tópicos incluem o software de comunicação serial, criando os arquivos de dispositivo serial, hardware serial, e configurando dispositivos seriais usando o `setserial` e `stty` comandos. Muitos outros temas são abordados em COMO FAZER Serial pelo advogado David.[26]

Software de comunicação para conexões de modem

Há uma série de pacotes de comunicação disponíveis para Linux. Muitos destes pacotes estão *terminal programas*, Que permitem ao usuário discar para outro computador como se estivesse sentado na frente de um terminal simples. A programa de terminal tradicional para os ambientes Unix-like é `kermit`. É, no entanto, bastante antiga agora, e provavelmente seria considerado difícil de usar. Existem vários programas disponíveis confortável que a FEA-suporte
ras, como dicionários de discagem telefônica, linguagens de script para automatizar a marcação e fazer login no computador remoto
sistemas, e uma variedade de protocolos de troca de arquivos. Um destes programas é `minicom`, Que foi modelado após alguns dos programas mais populares terminal DOS. usuários X11 são acomodados, também. `seyon` é caracterizado inteiramente
X11 baseado em programa de comunicações.

programas de terminal não são o único tipo de programas de comunicação serial disponível. Outros programas permitem que

você
conectar a um host e download de notícias e e-mail em um único pacote, para ler e responder mais tarde, em seu lazer. Este pode economizar muito tempo, e é especialmente útil se você tiver a infelicidade de viver em uma área onde seu local chamadas são cobradas de tempo. Todo o tempo lendo e respondendo pode ser gasto offline, e quando estiver pronto, você Pode remarcar e carregar suas respostas em um único pacote. Tudo isso consome um pouco de disco mais duro, porque todas as
as mensagens têm de ser armazenados no disco antes que você possa lê-los, mas este poderia ser um trade-off razoável na hoje é difícil elevar os preços.

UUCP exemplifica este estilo de software de comunicação. É um conjunto de programa que copia arquivos de um hospedeiro

para
outra e executa programas em um host remoto. É freqüentemente usado para o transporte de correio ou de notícias na rede privada de
obras. pacote de Ian Taylor UUCP, que também roda no Linux, é descrito em detalhes no Capítulo 16, *Gerir Taylor UUCP*. Outros softwares de comunicação não-interativas é utilizado através de redes, tais como Fidonet.
portos aplicação Fidonet como `ifmail` Também estão disponíveis, embora esperemos que não muitas pessoas ainda usam elas.

PPP e SLIP são entre eles, permitindo o uso interativo e não interativo. Muitas pessoas usam PPP ou SLIP
discar para a sua rede de campus ou de outros Internet Service Provider para executar FTP e ler páginas web. PPP e SLIP também são, no entanto, comumente usado em conexões permanentes ou semipermanentes para acoplamento de LAN-to-LAN, Embora este seja realmente interessante apenas com ISDN ou outras conexões de rede de alta velocidade.

Introdução aos dispositivos seriais

O kernel do Unix fornece dispositivos para acesso ao hardware serial, geralmente chamado de *tty* dispositivos (pronuncia-se como é

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

escrito: T-T-Y). Esta é uma abreviatura para *dispositivo de teletipo*, Que costumava ser um dos principais fabricantes de dispositivos terminais nos primeiros dias do Unix. O termo é usado agora para qualquer terminal de dados baseados em caracteres.
Ao longo deste capítulo, usamos o termo para referir-se exclusivamente ao dispositivo arquivos Linux ao invés do físico terminal.

Linux oferece três classes de dispositivos tty: Os dispositivos seriais, terminais virtuais (tudo o que você pode acessar, por sua

vez

apertando Alt-F1 até Alt-F*nn* na consola local), e pseudo-terminais (semelhante a um tubo de duas vias, usados por aplicativos como o X11). Os primeiros foram chamados de dispositivos tty porque o original terminais baseados em caracteres

[26] David pode ser contatado pelo bf347@lafn.org.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

estavam ligados à máquina Unix através de um cabo serial ou linha de telefone e modem. Os dois últimos foram nomeados após o dispositivo tty porque eles foram criados para se comportar de forma semelhante do ponto de vista do programador.

SLIP e PPP são mais comumente implementadas no kernel. O kernel realmente não tratam o *tty* dispositivo como um dispositivo de rede que pode ser manipulado como um dispositivo Ethernet, utilizando comandos como `ifconfig`. No entanto, ele faz tratamento dispositivos tty como locais onde os dispositivos de rede podem ser vinculados. Para fazer isso, as mudanças do kernel que está
chamado de "a disciplina da linha" do dispositivo tty. Ambos SLIP e PPP são disciplinas linha que pode ser ativado em tty dispositivos. A idéia geral é que o driver serial manipula os dados que lhe são dadas de forma diferente, dependendo da disci-line pline é configurado. Em sua disciplina linha padrão, o motorista simplesmente transmite cada personagem é dada em turno. Quando o PPP ou SLIP disciplina da linha for selecionada, o driver em vez lê um bloco de dados, envolve uma especial cabeçalho em torno dele que permite que o terminal remoto para identificar que bloco de dados em um riacho, e transmite os dados novos
bloco. Não é muito importante entender isso ainda, nós vamos cobrir tanto SLIP e PPP em capítulos posteriores, e tudo acontece automaticamente para você de qualquer maneira.

Acessando dispositivos Serial

Como todos os dispositivos em um sistema Unix, portas seriais são acessados através de arquivos especiais de dispositivo,

localizado na */ Dev* di-
tório. Há duas variedades de ficheiros de dispositivos relacionados aos motoristas de série, e não há um arquivo de dispositivo de cada tipo de
cada porta. O dispositivo irá se comportar de forma ligeiramente diferente, dependendo de qual dos seus ficheiros de dispositivos abrimos. Nós
cobrir a diferença porque ele vai ajudar você a entender algumas das configurações e conselhos que você pode
ver relativas aos dispositivos de série, mas na prática você precisará usar apenas um desses. Em algum ponto no futuro, uma eles podem até desaparecer completamente.

A mais importante das duas classes de dispositivo serial tem um maior número de 4, e seus arquivos de dispositivos são nomeado *ttyS0*,*ttyS1*, Etc variedade O segundo tem um maior número de 5, e foi projetado para uso ao discar para fora (Gritando) através de uma porta; seus arquivos de dispositivos são chamados *cua0*,*cua1*, Etc No mundo Unix, contagem geral-aliado começa em zero, enquanto os leigos tendem a começar por uma. Isso cria uma pequena quantidade de confusão para as pessoas se-
causa `COM1:` é representado por */ Dev/ttyS0*,`COM2:` por */ Dev/ttyS1*, Etc Alguém familiar com o IBM PC-style hard-ware sabe que `COM3:` e maior nunca foram realmente padronizados de qualquer maneira.

A *cua*, Ou "chamada", os dispositivos foram criados para resolver o problema de evitar conflitos de dispositivos seriais para mo-dems que têm de suportar tanto as conexões de entrada e de saída. Infelizmente, eles criaram a sua própria
problemas e são susceptíveis de ser interrompido. Vejamos brevemente o problema.

Linux, como o Unix, permite que um dispositivo, ou qualquer outro arquivo a ser aberto por mais de um processo

simultaneamente. Un-
Felizmente, isso raramente é útil com dispositivos tty, como os dois processos quase certamente interferem uns com os outras. Felizmente, um mecanismo foi concebido para permitir um processo para verificar se um dispositivo tty já tinha sido aberto pelo
outro dispositivo, antes de abri-lo. O mecanismo usa o que se chama *arquivos de bloqueio*. A idéia era que, quando um pro-ess queria abrir um dispositivo tty, seria verificar a existência de um arquivo em um local especial, um nome semelhante ao o dispositivo que pretende abrir. Se o arquivo não existir, o processo de cria e abre o dispositivo tty. Se o arquivo existir, o processo pressupõe um outro processo já tem o dispositivo tty aberto e toma as medidas apropriadas. Um truque passado para fazer o bloqueio de ficheiro de sistema de gestão foi escrito a identificação do processo (PID) do processo que havia criado o arquivo de bloqueio para o arquivo de bloqueio em si, vamos falar mais sobre isso em um momento.

O mecanismo de fechamento de arquivo funciona perfeitamente bem em circunstâncias em que você tem um local definido para

o fechamento
arquivos e todos os programas de saber onde encontrá-los. Infelizmente, isso nem sempre foi o caso do Linux. Não foi até o Linux Filesystem Standard definido um local padrão para arquivos de bloqueio quando *tty* arquivos de bloqueio começou a funcionar corretamente.
Ao mesmo tempo, havia pelo menos quatro, e os locais possivelmente mais escolhida pelos desenvolvedores de software para armazenamento de bloqueio
arquivos: */ Usr / spool / travas /*,*/ Var / spool / travas /*,*/ Var / lock / /*E */ Usr / lock / /*. A confusão provocou o caos. Os programas foram

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

abertura de arquivos de bloqueio em locais diferentes que foram feitos para controlar um dispositivo tty único, era como se os arquivos de bloqueio
não estavam sendo usados.

A *cua* dispositivos foram criados para fornecer uma solução para este problema. Em vez de depender do uso de arquivos de bloqueio para evitar conflitos entre os programas que desejam usar os dispositivos de série, foi decidido que o kernel pode fornecer um meio simples de arbitrar quem deve ter acesso. Se o *ttyS* dispositivo já estavam abertas, numa tentativa de abrir o *cua* resultaria em um erro que um programa pode interpretar no sentido de o dispositivo já estava sendo usado. Se o *cua* dispositivo já foram abertas e foi feita uma tentativa para abrir a *ttyS*, O pedido do bloco, ou seja, ele seria colocada em espera e esperar até que a *cua* dispositivo foi fechado por outro processo. Isso funcionou muito bem se você tinha um único modem que você tinha configurado para acesso dial-in e, ocasionalmente, queria discar em

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

mesmo dispositivo. Mas não funcionou muito bem em ambientes em que você tinha vários programas querendo chamar fora no mesmo dispositivo. A única maneira de resolver o problema de contenção era usar arquivos de bloqueio! De volta à estaca zero.

Basta dizer que o Linux Filesystem Standard veio para o resgate e agora determina que os arquivos sejam bloqueio armazenadas no */ Var / lock* diretório, e que, por convenção, o nome do arquivo de bloqueio para o *ttyS1* dispositivo, por exemplo, é
LCK .. ttyS1. A *cua* arquivos de bloqueio também deve ir neste diretório, mas o uso de *cua* dispositivos é desencorajado.

A *cua* dispositivos provavelmente ainda estarão por aí por algum tempo para proporcionar um período de compatibilidade com

versões anteriores, mas em
vez que eles serão aposentados. Se você está se perguntando o que usar, manter o *ttyS* dispositivo e certifique-se que o sis- Este sistema é compatível com Linux FSSTND, ou pelo menos que todos os programas que utilizam os dispositivos de série de acordo sobre onde
os arquivos de bloqueio estão localizados. A maioria dos softwares lidar com dispositivos tty serial fornece uma opção em tempo de compilação para especificar
a localização dos arquivos de bloqueio. Mais frequentemente do que não, isso vai aparecer como uma variável chamada algo como `LOCKDIR`
na *Makefile* ou em um arquivo de cabeçalho de configuração. Se você está compilando o software por si próprio, é melhor mudar isso de acordo com a localização FSSTND especificado. Se você estiver usando um binário pré-compilado e você não tiver certeza de onde
o programa irá gravar seus arquivos de trava, você pode usar o seguinte comando para obter uma dica:

```
strings binaryfile     | Grep bloqueio
```

Se o local encontrado não concorda com o resto do seu sistema, você pode tentar criar um link simbólico do Diretório de bloqueio que o executável estrangeiros quer de volta o uso */ Var / lock / /*. Isso é feio, mas ele irá trabalhar.

O dispositivo serial Arquivos Especiais

números menores são idênticas para ambos os tipos de dispositivos seriais. Se você tiver o modem em uma das portas COM1: COM4: o seu número menor será o número da porta COM mais 63. Se você estiver usando série especial hardware, como uma alta performance controlador de porta serial múltiplos, você provavelmente terá que criar especial arquivos do dispositivo para ele, ele provavelmente não vai usar o driver de dispositivo padrão. O Serial-HOWTO deve ser capaz de ajudar
-lo a encontrar as informações adequadas.

Assuma o seu modem está na COM2:. Seu número será menor de 65 anos, e sua maior número será de 4 para uso normal. Deve haver um dispositivo chamado *ttyS1* que tem esses números. Listar os ttys série no */ Dev /* diretório. O quinto e sexta colunas mostram os números maiores e menores, respectivamente:

```
$ ls-l / dev / ttyS *
0 crw-rw ----   1 uucp     dialout    4 º,           64 13 de outubro     1997 /
0 crw-rw ----   1 uucp     dialout    dev/ttyS0
0 crw-rw ----   1 uucp     dialout    4 º,  65 26 de janeiro 21:55 / dev/ttyS1
0 crw-rw ----   1 uucp     dialout    4 º,           66 13 de outubro     1997 /
                                      dev/ttyS2
                                      4 º,           67 13 de outubro     1997 /
                                      dev/ttyS3
```

Se não houver nenhum dispositivo com maior número 4 e número menor de 65 anos, você terá que criar um. Torne-se o super-ruser e digite:

```
#  mknod-m 666 / dev/ttyS1 c 4 65
#  chown uucp.dialout / dev/ttyS1
```

As várias distribuições Linux usam ligeiramente diferentes estratégias de que deve possuir os dispositivos de série. Some-vezes elas serão de propriedade da *root*, E outras vezes elas serão de propriedade de outro usuário, como uucp em nossa ex-amplo. distribuições modernas têm um grupo especificamente para os dispositivos dial-out, e os usuários que estão autorizados a utilizar
eles são adicionados a este grupo.

Algumas pessoas sugerem fazer */ Dev / modem* um link simbólico para o dispositivo de modem para que os usuários casuais não têm
para lembrar o pouco intuitivos *ttyS1*. No entanto, você não pode usar *modem* em um programa e de real nome do vice arquivo em outro. Seus arquivos de bloqueio que têm nomes diferentes e os mecanismo de bloqueio não de trabalho.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Hardware Serial

RS-232 é atualmente o padrão mais comum de comunicação serial no mundo PC. Ele usa uma série de
circuitos de transmissão de bits individuais, bem como para a sincronização. Outras linhas podem ser utilizados para sinalizar o presença de um transportador (utilizado pelos modems) e para handshaking. O Linux suporta uma grande variedade de cartões de série que
utilizam o padrão RS-232.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

handshake de hardware é opcional, mas muito útil. Ele permite que qualquer uma das duas estações para sinalizar se ele está pronto
para receber mais dados, ou se a outra estação deve esperar até que o receptor seja feito o processamento dos dados de entrada. As linhas utilizadas para isso são chamados de "Clear to Send (CTS) e" Ready to Send (RTS), respectivamente, ex-planícies o nome coloquial de handshake de hardware ". RTS / CTS" O outro tipo de aperto de mão que pode ser familiarizados com é chamado de "XON / XOFF" aperto de mão. XON / XOFF utiliza dois personagens nomeados, convencionalmente
Ctrl-C e Ctrl-Q, para sinalizar para o fim remoto que ele deve parar e começar a transmissão de dados, respectivamente. Enquanto
Este método é simples de implementar e aprovado para uso por terminais burros, que provoca uma grande confusão quando você está
lidar com dados binários, como você pode querer transmitir esses personagens como parte de seu fluxo de dados, e não ter los como caracteres de controle de fluxo. É também um pouco mais lento para ter efeito de handshake de hardware. handshake de hardware é limpo, rápido e recomendado em detrimento de XON / XOFF quando você tem uma escolha.

No IBM PC original, a interface RS-232 foi impulsionado por um chip chamado UART 8250. PCs em todo o tempo dos 486 usaram uma versão mais recente do chamado UART 16450. Foi um pouco mais rápido que o 8250. Quase todos máquinas Pentium tenham sido fornecidos com uma versão ainda mais recente do chamado UART 16550. Alguns marcas (principalmente modems internos equipados com o chip Rockwell set) usam chips completamente diferentes que emular o comportamento dos 16.550 e pode ser tratada da mesma forma. O Linux suporta todos estes na sua série padrão driv portoer.[27]

O 16550 foi uma melhoria significativa em relação a 8250 e os 16450 porque ele ofereceu um buffer de 16 bytes FIFO. O 16550 é realmente uma família de dispositivos de UART, compreendendo o 16550, 16550A, eo 16550AFN (mais tarde renomeado PC16550DN). As diferenças referem-se se o FIFO realmente funciona, o 16550AFN é o que é certo para o trabalho. Houve também um NS16550, mas a sua FIFO nunca trabalhou tanto.

O UARTs 8250 e 16450 tiveram um buffer simples de 1 byte. Isso significa que um 16.450 gera uma interrupção para cada caractere transmitido ou recebido. Cada interrupção tem um curto período de tempo de serviço, e essa pequena atraso limites 16450s para uma velocidade máxima pouco confiável de cerca de 9.600 bps em uma máquina típica barramento ISA.

Na configuração padrão, o kernel verifica o padrão de quatro portas seriais, COM1 a COM4:. O kernel também é capaz de detectar automaticamente o UART é usada para cada uma das portas seriais padrão, e fará uso de o FIFO buffer maior do 16550, se ele estiver disponível.

Usando os utilitários de configuração

Agora vamos passar algum tempo olhando para os dois mais úteis utilitários de configuração de série do dispositivo:

`setserial` e
`stty`.

O comando setserial

O kernel irá envidar seus melhores esforços para determinar corretamente quanto seu hardware serial está configurada, mas o va-ções sobre a configuração do dispositivo serial faz essa determinação difícil de alcançar 100 por cento confiável na prática. Um bom exemplo de que este é um problema é o modem interno de que falamos anteriormente. O UART eles usam tem um buffer de 16 bytes FIFO, mas parece que um UART 16450 para o driver de dispositivo do kernel: a menos que diga especificamente
o driver que esta porta é um dispositivo de 16550, o kernel não fará uso da reserva estendida. No entanto, outra ex-ampla é que as cartas mudo de 4 portas que permitem o compartilhamento de um único IRQ entre vários dispositivos seriais. Nós
poderá ter de dizer especificamente o kernel que porta IRQ que deveria usar, e que IRQs podem ser compartilhadas.

`setserial` foi criado para configurar o driver serial durante a execução. A `setserial` comando é mais com-comumente executadas em tempo de inicialização de um script chamado *0setserial* em algumas distribuições, e *rc.serial* sobre os outros. Este
script está com a responsabilidade de inicialização do driver serial para acomodar qualquer fora do padrão ou não-hardware serial sempre na máquina.

A sintaxe geral para o `setserial` comando é:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`setserial` *dispositivo* [*parâmetros*]
em que o dispositivo é um dos dispositivos seriais, como *ttyS0*.

27 Note que não estamos falando de WinModem (TM) aqui! WinModems tem hardware muito simples e confiar totalmente na principal hardware da CPU do seu computador ao invés de dedicado a fazer todo o trabalho duro. Se você está comprando um modem, ele é o nosso forte consdação para *não* compra um modem desse tipo, ter um modem real. Você pode encontrar suporte para Linux WinModems, mas que faz com que eles apenas uma solução ligeiramente mais atraente.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A `setserial` comando tem um grande número de parâmetros. Os mais comuns são descritas na Tabela 4.1.Para obter informações sobre o restante dos parâmetros, você deve consultar o `setserial` manual
página.

Tabela 4.1: setserial Command Line Parameters

Parâmetro	Descrição
`porto` *port_number*	Especifique o endereço de I / O da porta serial dispositivo. Os números de porta deve ser especificado em notação hexadecimal, por exemplo, `0x2f8`.
`irq` *Num.*	Especifique a linha de solicitação de interrupção do dispositivo serial está usando.
`uart` *uart_type*	Especifique o tipo de UART do dispositivo serial. Os valores comuns são `16450`,`16550`, Etc Definir esse valor para `none` irá desabilitar este dispositivo serial.
`Fourport`	A especificação desse parâmetro instrui o kernel driver serial que esta porta é uma porta de uma placa AST Fourport.
`spd_hi`	Programa do UART para usar uma velocidade de 57,6 kbps quando um processo solicita 38,4 kbps.
`spd_vhi`	Programa do UART para usar uma velocidade de 115 kbps, quando um processo solicita 38,4 kbps.
`spd_normal`	Programa do UART para usar o padrão de velocidade de 38,4 kbps, quando solicitado. Esta parâmetro é usada para reverter o efeito de uma `spd_hi` ou `spd_vhi` realizada no especificado dispositivo serial.
`auto_irq`	Este parâmetro fará com que o kernel para tentar determinar automaticamente o IRQ o dispositivo especificado. Essa tentativa pode não ser totalmente confiável, por isso é provavelmente melhor pensar nisso como um pedido para o kernel para adivinhar o IRQ. Se você souber o IRQ do dispositivo, você deve especificar que ele use o `irq` parâmetro em vez.
`autoconfig`	Este parâmetro deve ser especificado em conjunto com o `porto` parâmetro. Quando isso parâmetro for fornecido, `setserial` instrui o kernel para tentar automaticamente determinar o tipo de UART localizado no endereço de porta fornecido. Se o `auto_irq` parâmetro também é fornecido, o kernel tenta determinar automaticamente o IRQ, também.
`skip_test`	Este parâmetro instrui o kernel para não incomodar a realização do ensaio do tipo UART dução auto-configuração. Isso é necessário quando o UART é incorretamente detectado pelo o kernel.

Um típico e simples *rc* arquivo para configurar as portas seriais em tempo de inicialização poderia ser algo como o mostrado na Exemplo 4.1. A maioria das distribuições Linux inclui algo um pouco mais sofisticado do que este.

Exemplo 4.1: Comandos setserial Exemplo rc.serial

```
# / Etc / rc.serial - script de configuração de série da linha.
#
# Configurar dispositivos seriais
/ Sbin / setserial / dev/ttyS0 skip_test auto_irq autoconfig
/ Sbin / setserial / dev/ttyS1 skip_test auto_irq autoconfig
/ Sbin / setserial / dev/ttyS2 skip_test auto_irq autoconfig
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
/ Sbin / setserial / dev/ttyS3 skip_test auto_irq autoconfig
#
# Mostra a configuração do dispositivo serial
/ Sbin / bg-setserial / dev / ttyS *
```

A `-Bg / dev / ttyS *` argumento do último comando irá imprimir um resumo perfeitamente formatado do hardware configuração de todos os dispositivos ativos em série. O resultado será parecido com o mostrado na Exemplo 4.2.

Exemplo 4.2: Saída do BG-setserial / dev / ttyS Comando

```
/ Dev/ttyS0 no 0x03f8 (irq = 4) é um 16550A
```

/ Dev/ttyS1 na 0x02f8 (irq = 3) é um 16550A

O comando stty

O nome `stty` provavelmente significa "tty set", mas o `stty` comando também pode ser usado para exibir um terminal de configuração. Talvez até mais do que `setserial`, O `stty` comando fornece um número impressionante de características que você pode configurar. Nós vamos cobrir o mais importante desses em um momento. Você pode encontrar o resto descrito no `stty` manual de página.

A `stty` comando é mais comumente usado para configurar os parâmetros de terminal, como se os personagens vão seja exibido ou qual tecla deve gerar um sinal de interrupção. Nós explicamos anteriormente que os dispositivos de série são dispositivos tty e o `stty` comando é igualmente aplicável a eles.

Um dos usos mais importantes do `stty` para dispositivos seriais é permitir handshaking de hardware do dispositivo. Conversamos um pouco sobre o hardware handshaking anterior. A configuração padrão para dispositivos seriais é para hardware handshaking para ser desativada. Esta configuração permite que "três fios" cabos seriais para trabalhar, pois eles não suportam a sinais necessários para handshaking de hardware, e se fosse ativado por padrão, que seria incapaz de transmitir qualquer caracteres para mudar isso.

Surpreendentemente, alguns programas de comunicação serial não permitem handshaking de hardware, portanto, se seu modem suportos handshaking de hardware, você deve configurar o modem para usá-lo (confira o manual do modem para o que comando para usar), e também configurar o seu dispositivo serial para usá-lo. A `stty` comando tem uma `crtscts` bandeira que habilita handshaking de hardware em um dispositivo, você vai precisar usar isso. O comando é provavelmente o melhor emitidos a partir de o *rc.serial* arquivo (ou equivalente) em tempo de inicialização usando comandos como os mostrados na Exemplo 4.3.

Exemplo 4.3: Exemplo de comandos stty rc.serial

```
#
stty crtscts </ dev/ttyS0
stty crtscts </ dev/ttyS1
stty crtscts </ dev/ttyS2
stty crtscts </ dev/ttyS3
#
```

A `stty` comando funciona no terminal atual por padrão, mas usando o recurso de redirecionamento de entrada de ("<") a casca, que pode ter `stty` manipular qualquer dispositivo tty. É um erro comum esquecer se você é supque representam para a utilização "<" ou ">"; versões modernas da `stty` comandos têm uma sintaxe muito mais limpa para fazer isso. Para usar a nova sintaxe, nós reescrever o nosso exemplo de configuração para olhar como o mostrado na Exemplo 4.4.

Exemplo 4.4: Exemplo rc.serial Comandos stty utilizando modernas Sintaxe

```
#
stty crtscts F / dev/ttyS0
stty crtscts F / dev/ttyS1
stty crtscts F / dev/ttyS2
stty crtscts F / dev/ttyS3
#
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Nós mencionamos que o `stty` comando pode ser usado para exibir os parâmetros de configuração de um terminal tty dispositivo. Para exibir todas as configurações de ativos em um dispositivo tty, use:

```
$ stty-a-F / dev/ttyS1
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A saída deste comando, mostrada na Exemplo 4.5,dá-lhe o status de todas as bandeiras para esse dispositivo, uma bandeira mostrada com um sinal de menos precedente, como em *-Crtscts*, Significa que a bandeira foi desativada.

Exemplo 4.5: Saída do comando stty-a

```
velocidade de 19200 baud; linhas 0, colunas 0, linha = 0;
intr = C ^; sair ^ = \; apagar = ^;? matar ^ U =; eof = D ^; eol = <undef>;
         eol2 = <undef>; start = ^ Q; parar = S ^; susp = ^ Z; rprint = ^ R;
         min = 1;; werase = W ^; lnext = V ^; flush = ^ O tempo = 0;
-Parenb-parodd cs8 cread cstopb hupcl-clocal-crtscts
-Ignbrk-BRKINT-ignpar-PARMRK-inpck-istrip-inlcr-IGNCR-ixon-icrnl
        -Ixoff-iuclc-ixany-imaxbel
-OPOST-olcuc-ocrnl onlcr-onocr-onlret-OFILL-ofdel NL0 cr0 tab0
         BS0 VT0 ff0
IEXTEN-ISIG icanon-eco ecoam echoe-ECHONL-NOFLSH-xcase-tostop
         -Echoprt ECHOCTL ECHOKE
```

A descrição dos mais importantes desses sinalizadores é dada em Tabela 4.2.Cada um desses sinalizadores é ativado por oferta ção para `stty` e pessoas com deficiência, fornecendo-a para `stty` com o caracter - em frente a ela. Assim, para desabilitar o hardware
handshaking na `ttyS0` dispositivo, você usaria:

```
$ stty-crtscts F / dev/ttyS0
```

Tabela 4.2: Bandeiras stty mais relevantes para configurar dispositivos seriais

Bandeiras	Descrição
`N`	Definir a velocidade da linha para `N` bits por segundo.
`crtsdts`	Activar / Desactivar handshaking de hardware.
`ixon`	Activar / Desactivar controle por XON / XOFF.
`clocal`	Activar / Desactivar os sinais de controle de modem, como DTR / DCD e DTS. Isto é necessário Se você estiver usando um "três fios" cabo serial, pois não fornecem estes sinais.
`CS5 CS6 CS7 cs8`	Definir o número de bits de dados a 5, 6, 7 ou 8, respectivamente.
`parodd`	Habilitar paridade ímpar. A desativação desse indicador permite ainda a paridade.
`parenb`	Ativar verificação de paridade. Quando esse sinalizador é negada, sem paridade é usada.
`cstopb`	Possibilitar a utilização de dois bits de paragem por personagem. Quando esse sinalizador é negado, por um bit de parada
`echo`	caractere é usado. Activar / Desactivar eco dos caracteres recebidos de volta ao remetente.

O exemplo seguinte combina algumas dessas bandeiras e define o *ttyS0* dispositivo para 19.200 bps, 8 bits de dados, sem paridade,
handshaking de hardware e com o eco com deficiência:

```
$stty 19200 cs8-parenb crtscts-eco-F / dev/ttyS0
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Os dispositivos seriais eo prompt de login:

Era uma vez que é muito comum que uma instalação Unix envolvidos uma máquina servidor e muitas personagem "burra" terminais modo ou modems dial-up. Hoje esse tipo de instalação é menos comum, que é uma boa notícia para muitos pessoas interessadas em operar desta maneira, porque o "burro" terminais são muito baratos de adquirir. Dial-up configurações do modem não são menos comuns, mas estes dias que provavelmente seria usado para apoiar um ou SLIP PPP login (discutido no Capítulo 7, *Serial Line IP* eo capítulo 8, *O protocolo ponto-a-Ponto*Que) para ser usado um login simples. No entanto, cada uma dessas configurações podem fazer uso de um programa simples chamado `getty` programa.

O termo `getty` é provavelmente uma contração de "pegar o terminal." A `getty` programa abre um dispositivo serial, configura-
apropriadamente, opcionalmente, configura um modem, e aguarda uma conexão seja feita. Uma conexão ativa em um dispositivo serial normalmente é indicado pelo Data Carrier Detect pino (DCD) sobre o dispositivo serial que está sendo gerado. Quando um
conexão é detectado, o `getty` programa emite uma `login:` prompt, e então chama o `login` programa para lidar com o login do sistema real. Cada um dos terminais virtuais (por exemplo, */ Dev/tty1*) No Linux tem um `getty` execução contra ele.

Há um número de diferentes `getty` implementações, cada uma adequada para algumas configurações melhores do que os outros. A `getty` que iremos descrever aqui é chamado `mgetty`. É muito popular porque tem todos os tipos de ca-estruturas que o tornam especialmente modem-friendly, incluindo suporte para programas de fax e modems de voz automática. Vamos nos concentrar sobre a configuração `mgetty` para atender chamadas de dados convencionais e deixar o resto para você explorar a sua conveniência.

Configurando o Daemon mgetty

A `mgetty` daemon está disponível em forma de fonte de ftp://alpha.greenie.net/pub/mgetty/source/,e está disponível poder em quase todas as distribuições Linux em forma pré-embalada. A `mgetty` daemon difere da maioria dos outros `getty` implementações em que foi projetado especificamente para os modems compatíveis com Hayes. Ele ainda suporta conexões do terminal direto, mas é mais adequado para aplicações de dial-up. Ao invés de usar a linha DCD para detectar uma chamada recebida, ela ouve o `ANEL` mensagem gerada por modems modernos quando detectar uma chamada e não estão configurados para auto-resposta.

O programa executável principal é chamado */ Usr / sbin / mgetty*E seu arquivo de configuração principal é chamado */ Etc / mgetty / mgetty.config*. Há uma série de outros programas binários e arquivos de configuração que abrangem outras `mgetty` recursos.

Para a maioria das instalações, configuração é uma questão de edição o */ Etc / mgetty / mgetty.config* ade arquivo e adicionando-entradas adequadas para o */ Etc / inittab* arquivo para executar `mgetty` automaticamente.

Exemplo 4.6 shoFoi uma forma muito simples `mgetty` arquivo de configuração. Este exemplo configura dois dispositivos seriais. A
em primeiro lugar, */ Dev/ttyS0*, Suporta um modem compatível com Hayes em 38.400 bps. A segunda, */ Dev/ttyS0*, Uma apoia directamente
ligada ao terminal VT100 19.200 bps.

Exemplo 4.6: Exemplo de / etc / mgetty / mgetty.config Arquivo

```
#
# Arquivo de configuração do mgetty
#
# Isto é um arquivo de configuração de exemplo, consulte mgetty.info para detalhes
#
linhas de comentário # começar com um "#", linhas vazias são ignoradas
#
# Seção ----- ----- global
#
# Nesta seção, você coloca os padrões globais, por material de porta está abaixo
#
# Acesso ao modem (s) com 38.400 bps
velocidade de 38400
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
#
# Definir o nível de depuração global "4" (padrão de policy.h)
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
depuração 4
#

# Seção específica ----- ----- porto
#
# Aqui você pode colocar as coisas que são válidas apenas para uma linha, e não os
outros
#
#
# Hayes modem conectado a ttyS0: não faça fax, menos o log
#
porta ttyS0
  depuração 3
  somente de dados y
#
# Conexão direta de um terminal VT100, que não gosta cai DTR
#
porta ttyS1
  y directo
  velocidade de 19200
  dtr alternar-n
#
```

O arquivo de configuração global e oferece suporte a opções específicas do port. No nosso exemplo usamos uma opção global

para definir
a velocidade de 38.400 bps. Este valor é herdado pelos *ttyS0* porto. Portas que se aplicam `mgetty` para usar este conjunto de velocidade
ting, a menos que seja substituído por uma configuração de velocidade da porta específicos, como fizemos no *ttyS1* configuração.

A `depurar` palavra-chave controla a verbosidade `mgetty` madeireira. A `somente de dados` palavra-chave na *ttyS0* configuração causas `mgetty` para ignorar quaisquer recursos de fax modem, para funcionar como um modem de dados. A `directo`
palavra-chave na *ttyS1* configuração instrui `mgetty` não a qualquer tentativa de inicialização do modem na porta. Finalmente, a `dtr-toggle` palavra-chave instrui `mgetty` não tentar desligar a linha, deixando de lado o DTR
(Data Terminal Ready), pino da interface serial, alguns terminais não gosto que isso aconteça.

Você também pode optar por deixar o *mgetty.config* arquivo vazio e use argumentos de linha de comando para especificar a

maioria dos
os mesmos parâmetros. A documentação que acompanha o pedido inclui uma descrição completa do
`mgetty` parâmetros de configuração do arquivo e argumentos de linha de comando. Veja o exemplo a seguir.

Precisamos adicionar duas entradas para o */ Etc / inittab* arquivo para ativar esta configuração. A *inittab* arquivo é a

configuração-
ção de arquivos do Sistema Unix V `init` comando. A `init` comando é responsável pela inicialização do sistema, que fornece um meio de executar automaticamente os programas em tempo de inicialização e re-executá-los quando terminar. Isto é ideal para as metas de execução de um `getty` programa.

```
T0: 23: respawn: / sbin / mgetty ttyS0
T1: 23: respawn: / sbin / mgetty ttyS1
```

Cada linha do */ Etc / inittab* arquivo contém quatro campos, separados por vírgulas. O primeiro campo é um identificador que exclusivamente etiquetas uma entrada no arquivo; tradicionalmente é dois personagens, mas as versões modernas permitem quatro. A segunda
campo é a lista de níveis de execução em que essa entrada deve estar ativa. Um nível de execução é um meio alternativo de fornecer
configurações da máquina e é implementado usando árvores de scripts de inicialização armazenadas em diretórios chamados */ Etc/rc1.d*,
/ Etc/rc2.d, Etc Este recurso normalmente é implementado de forma muito simples, e você deve modelar as entradas em outros em
o arquivo ou consulte a documentação do sistema para obter mais informações. O terceiro campo descreve quando tomar ação. Para efeitos de execução de um `getty` programa, este campo deve ser ajustado para `respawn`, Significando que o comando deve ser re-executado automaticamente quando ele morre. Existem várias outras opções, bem como, mas eles são não é útil para nossos propósitos. O quarto campo é o comando real para executar, que é onde especificamos o

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`mgetty` comando e quaisquer argumentos que queremos passar. No nosso exemplo simples que estamos começando e reiniciando
`mgetty` sempre que o sistema está operando em um dos níveis de execução de dois ou três, e estamos fornecendo como argumento
apenas o nome do dispositivo que desejamos usar. A `mgetty` assume o comando */ Dev /*, Por isso não precisa fornecê-lo.

Este capítulo foi uma rápida introdução `mgetty` e como a oferta de login pede para dispositivos seriais. Você pode encontrar informações mais detalhadas do Serial-HOWTO.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Depois de ter editado os arquivos de configuração, você precisará recarregar `init` para fazer as alterações tenham efeito. Basta enviar um sinal de desligar a `init` processo, mas sempre tem um processo de identificação de um, assim você pode usar o seguinte com-
mando de forma segura:

```
# kill-HUP 1
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 5 - Configurando o TCP / IP

Neste capítulo, vamos orientá-lo através de todos os passos necessários para configurar a rede TCP / IP em sua máquina. Start-
ção com a atribuição de endereços IP, lentamente trabalhar o nosso caminho através da configuração de rede TCP / IP
interfaces e apresentar algumas ferramentas que vêm a calhar quando caçando problemas de instalação de rede.

A maioria das tarefas descritas neste capítulo em geral tem de ser feito apenas uma vez. Depois, você tem que tocar
a maioria dos arquivos de configuração somente quando a adição de um novo sistema para sua rede ou quando você reconfigurar o seu sistema
inteiramente. Alguns dos comandos usados para configurar o TCP / IP, no entanto, para ser executado cada vez que o sistema inicializado. Isso geralmente é feito invocando-los do sistema */ * / Etc / rc* scripts.

Normalmente, a parte de rede específicos deste procedimento está contida em um script. O nome deste script varia de
diferentes distribuições de Linux. Em muitas distribuições Linux mais antigas, ela é conhecida como *rc.net* ou *rc.inet*. Às vezes você
também vai ver dois scripts chamado *rc.inet1* e *rc.inet2*, O ex-inicializa a parte do kernel do trabalho em rede ea
A última inicia serviços básicos de rede e aplicações. Em distribuições modernas, o *rc* arquivos são estruturados em um
arranjo mais sofisticado, aqui você pode encontrar scripts no */ Etc / init.d /* (Ou */ Etc / rc.d / init.d /*) Diretório que
criar os dispositivos de rede e outros *rc* arquivos que são executados os programas de aplicação de rede. exemplos deste livro são com base no último arranjo.

Este capítulo aborda as partes do script que configura as interfaces de rede, enquanto as candidaturas serão abran-
rado em capítulos posteriores. Depois de terminar este capítulo, você deve ter estabelecido uma seqüência de comandos que configurar corretamente a rede TCP / IP em seu computador. Você deve, então, substituir os comandos de exemplo na
scripts de configuração com os seus comandos, certifique-se que o script é executado a partir da base *rc* script em
tempo de inicialização e reiniciar a máquina. A ligação em rede *rc* scripts que vêm junto com o seu favorito Linux dis-
tribuição deve fornecer um exemplo sólido de que para trabalho.

Montando o sistema de arquivos / proc

Algumas das ferramentas de configuração do Linux NET-2 e NET-3 dependem da liberação */ Proc* sistema de arquivos para

comu-
nicar com o kernel. Esta interface permite o acesso à informação em tempo de execução do kernel através de um sistema de arquivos como
mecanismo. Quando montado, você pode listar seus arquivos como qualquer outro sistema de arquivos, ou exibir seu conteúdo. Típica
itens incluem o *loadavg* arquivo, que contém a média de carga do sistema e *meminfo*, Que mostra o núcleo actual
memória e uso de swap.

Para isso, o código de rede adiciona o *net* diretório. Ele contém uma série de arquivos que mostram coisas como o kernel
tabelas ARP, o estado das conexões TCP, e as tabelas de roteamento. A maioria das ferramentas de administração de rede obter a sua
informações a partir desses arquivos.

A *proc* sistema de arquivos (ou *procfs*, Como também é conhecido) é montada */ Proc* em tempo de inicialização do sistema. O

melhor
método é adicionar a seguinte linha */ Etc / fstab*:

```
procfs # ponto de montagem:
none            / Proc          proc    padrões
```

Em seguida, execute `mount / proc` a partir do seu */ Etc / rc* script.

A *procfs* agora está configurado para a maioria dos kernels por padrão. Se o *procfs* não está em seu kernel, você terá um show-
sábio, tais como: `mount: tipo de fs procfs não suportado pelo kernel`. Você terá então de reco-
pilha do kernel e responder "sim" quando perguntado sobre *procfs* apoio.

Instalar os binários

Se você estiver usando uma das distribuições Linux pré-embalados, que conterá as principais aplicações de redes
utilitários. Juntamente com um conjunto coerente de arquivos de exemplo. O único caso em que poderá ter de obter e in-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

stall novos utilitários é quando você instala uma nova versão do kernel. Como eles ocasionalmente envolver alterações no kernel camada de rede, você precisará atualizar as ferramentas de configuração básica. Essa atualização, no mínimo, envolve-recompil ção, mas às vezes você também pode ser necessária para obter o último conjunto de binários. Estes binários estão disponíveis em seu site oficial em casa ftp.inka.de / pub / comp / Linux / networking / NetTools /,empacotados em um arquivo chamado *net-ferramentas de XXX.tar.gz*, Onde *XXX* é o número da versão. A versão 2.0 é compatível Linux *net-tools-1,45*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Se você quiser compilar e instalar o padrão TCP / IP aplicações de rede mesmo, você pode obter as fontes da maioria dos servidores FTP Linux. Todas as distribuições Linux modernas incluem uma gama bastante completa de TCP / IP aplicações de rede, tais como navegadores da World Wide Web, `telnet` e `ftp` programas e aplicações de rede outras cátions, tais como `Discussão`. Se você encontrar algo que você precisa para compilar a si mesmo, as chances são boas que ele irá compilar no Linux de fonte pura e simplesmente, se você seguir as instruções incluídas no pacote de código-fonte idade.

Definir o nome do host

A maioria, senão todas, as aplicações de rede confiar em você para definir o nome do host local para um valor razoável. Este configuração normalmente é feita durante o processo de inicialização, executando o `hostname` comando. Para definir o nome do host
para *nome*, Digite:

```
# hostname   nome
```

É prática comum usar o nome da máquina não qualificado, sem especificar o nome de domínio. Por exemplo, os hosts na Cervejaria Virtual (descrito no Apêndice A, *Rede Exemplo: A Cervejaria Virtual*) Pode ser chamado *vale.vbrew.com* ou *vlager.vbrew.com*. Estes são os seus oficiais *nomes de domínio totalmente qualificado* (FQDNs). Sua local hostnames seria o primeiro elemento do nome, como *Vale*. No entanto, como o host local é freqüentemente usado para procurar o endereço IP do host, você tem que ter certeza que a biblioteca de resolução é capaz de olhar para cima do anfitrião
Endereço IP. Isso normalmente significa que você tem que digitar o nome no */ Etc / hosts*.

Algumas pessoas sugerem o uso do `domainname` comando para definir idéia do kernel de um nome de domínio para os restan- ção parte do FQDN. Desta forma, você pode combinar a saída do `hostname` e `domainname` para obter o FQDN novamente. No entanto, esta é a melhor em apenas meio correto. `domainname` é geralmente usado para definir o NIS do hospedeiro
domínio, que pode ser totalmente diferente do domínio DNS ao qual o host pertence. Em vez disso, para assegurar que a forma abreviada de seu nome do host é resolvido com todas as versões recentes do `hostname` comando, adicioná-lo como uma entrada no seu local Domain Name Server ou colocar o nome de domínio totalmente qualificado no */ Etc / hosts*
arquivo. Você pode então usar o *- Fqdn* argumento para o `hostname` comando, e ele irá imprimir o totalmente qualificados do- nome principal.

Atribuindo endereços IP

Se você configurar o software de rede em seu computador para operação autônoma (por exemplo, para ser capaz de executar da DCI software Netnews), você pode seguramente pular esta seção, porque o único endereço IP que você precisa é para o interface de loopback, que é sempre *127.0.0.1*.

As coisas estão um pouco mais complicado com as redes reais, como a Ethernet. Se você quiser ligar o anfitrião de uma existentes na rede, você tem que perguntar a seus administradores para lhe dar um endereço IP nesta rede. Ao configurar um rede sozinho, você tem que atribuir endereços IP a si mesmo.

Hosts em uma rede local deve normalmente compartilham os endereços da mesma rede IP lógica. Assim, você tem para atribuir um endereço IP de rede. Se você tiver várias redes físicas, você tem que quer atribuir-lhes diferentes números de rede, ou uso de sub-rede para dividir o intervalo de endereços IP em várias sub-redes. Sub-rede será revisitados na próxima seção, "Criando sub-redes".

Ao escolher um número de rede IP, depende muito se você pretende entrar na Internet no próximo futuro. Se assim for, você deve obter um endereço IP oficial *agora*. Pergunte ao seu provedor de serviços de rede para ajudá-lo. Se você
deseja obter um número de rede, apenas no caso você pode entrar na Internet um dia, pedir um endereço de rede Formulário de Candidatura da hostmaster@internic.net, ou o seu próprio país Network Information Center, se houver um.

Se a rede não estiver conectado à Internet e não será num futuro próximo, você é livre para escolher qualquer questão legal endereço de rede. Apenas certifique-se que nenhum pacote da sua rede interna de fuga à Internet real. Para certificar-se nenhum dano pode ser feito mesmo se os pacotes *fez* escapar, você deve usar um dos números de rede reservados para uso privado
uso. A Internet Assigned Numbers Authority (IANA) reservou vários números de rede das classes A,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

B e C que você pode usar sem se cadastrar. Esses endereços são válidos apenas dentro da rede privada e não são roteadas entre sites da Internet real. Os números são definidos pela RFC 1597 e estão listadas na Tabela 2.1 em

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 2, *Problemas de rede TCP / IP*. Observe que o segundo e terceiro blocos que contêm 16 e 256 redes, , respectivamente.

Escolher seus endereços de um destes números de rede não é útil apenas para as redes completamente

inconscientes,
conectado à Internet, você ainda pode aplicar um acesso um pouco mais limitada usando um único host como um gateway. Para sua rede local, o gateway pode ser acessado pelo endereço IP interno, enquanto o mundo lá fora sabe que por um endereço oficial registrado (atribuído a você pelo seu provedor). Voltamos a este conceito em conexão com a instalação de IP masquerade no Capítulo 11, *IP Masquerade e Network Address Translation*.

Durante todo o restante do livro, vamos supor que o gerente da cervejaria rede usa uma classe B-net número do trabalho, digamos *172.16.0.0*. Naturalmente, um número de rede classe C com certeza gostaria de ser suficiente para acomodar
tanto da cervejaria e redes da vinícola. Vamos usar uma rede de classe B aqui em prol da simplicidade, que irá tornar os exemplos de sub-rede na próxima seção deste capítulo um pouco mais intuitiva.

Criar sub-redes

Para operar Ethernets diversas (ou outras redes, uma vez que um motorista está disponível), você tem que dividir sua rede em sub-redes. Note-se que a sub-rede é necessária somente se você tiver mais de um *rede de transmissão* - Ponto-a-ponto links não contam. Por exemplo, se você tiver uma Ethernet, e uma ou mais ligações SLIP para o mundo exterior, você não necessitam de sub-rede. Isto é explicado em detalhes no Capítulo 7, *Serial Line IP*.

Para acomodar os dois Ethernets, gerente da cervejaria rede decide usar 8 bits da parte de acolhimento, como adicionais bits de sub-rede. Isto deixa mais 8 bits para a parte de host, permitindo a 254 hosts em cada uma das sub-redes. Ela atribui um número de sub-rede para a cervejaria, e dá o número 2 da adega. A sua rede de anúncios respec- vestidos são assim *172.16.1.0* e *172.16.2.0*. A máscara de sub-rede é *255.255.255.0*.

vlager, Que é a passagem entre as duas redes, é atribuído um número de série de um dos dois deles, que dá-lhe os endereços IP *172.16.1.1* e *172.16.2.1*, Respectivamente.

Note que neste exemplo estamos usando uma rede de classe B para manter as coisas simples, mas uma rede de classe C seria mais realista. Com o novo código de rede, sub-redes não se limita a byte limites, por isso mesmo a classe C rede pode ser dividida em várias sub-redes. Por exemplo, você poderia usar dois bits da parte de host para a máscara, dando-lhe quatro possíveis sub-redes com 64 hosts em cada um.[28]

Escrita e arquivos hosts das redes

Depois de ter sub-rede, você deve se preparar para algum tipo simples de resolução de nomes usando o */ Etc / hosts* arquivo. Se você não está indo para usar DNS ou NIS para resolução de endereços, você tem que colocar todos os hosts no
hosts arquivo.

Mesmo se você deseja executar DNS ou NIS durante a operação normal, você deve ter um subconjunto de todos os hosts em */ Etc / hosts*. Você deve ter algum tipo de resolução de nomes, mesmo quando não há interfaces de rede estão funcionando, para exemplo, durante a inicialização. Este não é apenas uma questão de conveniência, mas permite que você use hostnames simbólica
em sua rede *rc* scripts. Assim, ao alterar os endereços IP, você só tem que copiar uma actualização *hosts* arquivo para todos máquinas e reiniciar, em vez de editar um grande número de *rc* arquivos separadamente. Normalmente você colocar todos os hosts locais
e aborda, em *hosts*, Somando os de qualquer gateways e servidores NIS usado.[29]

Você deve se certificar do seu resolvedor utiliza apenas a informação do *hosts* arquivo durante o teste inicial. Exemplo de

arquivos
que vêm com o software de DNS ou NIS pode produzir resultados estranhos. Para fazer com que todas as aplicações de uso */ Etc / hosts*
exclusivamente, ao procurar o endereço IP de um host, você tem que editar o */ Etc / host.conf* arquivo. Comente qualquer linhas que começam com a palavra-chave *fim* precedendo-os com um cardinal, e inserir a linha:

```
order hosts
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

28 O primeiro número em cada sub-rede é o endereço de sub-rede eo último número em cada sub-rede é reservado como o endereço de broadcast, de modo é realmente 62 hosts por subrede.

29 Você precisa do endereço de um servidor NIS se você usa o NYS Peter Eriksson. Outras implementações NIS localizar seus servidores somente no tempo de execução usando `ypbind`.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A configuração da biblioteca de resolução é abordado em detalhes no Capítulo 6, *Serviço de Nome e Resolver Configuração*.

A *hosts* arquivo contém uma entrada por linha, que consiste em um endereço IP, hostname, e uma lista de opcionais de aliases para o hostname. Os campos são separados por espaços ou tabulações, e no campo de endereço deve começar na primeira coluna.
Qualquer coisa que segue um cardinal (#) é considerado um comentário e é ignorado.

Nomes de host pode ser totalmente qualificado ou relativo para o domínio local. Para *Vale*, Você normalmente entra a nome totalmente qualificado, *vale.vbrew.com*E *Vale* por si só na *hosts* arquivo, assim que é conhecido por seus dois oficiais nome eo nome mais curto local.

Este é um exemplo de como um *hosts* arquivo na Cervejaria Virtual pode olhar. Dois nomes especiais estão incluídos, *vlager-if1* e *vlager-if2*, Que dá os endereços para as interfaces utilizadas em *vlager*:

```
#
# Arquivo hosts do Virtual Cervejaria / Virtual Winery
#
# IP            FQDN                aliases
#
127.0.0.1       localhost
#
172.16.1.1      vlager.vbrew.com      vlager vlager-if1
172.16.1.2      vstout.vbrew.com      vstout
172.16.1.3      vale.vbrew.com        Vale
#
172.16.2.1      vlager-if2
172.16.2.2      vbeaujolais vbeaujolais.vbrew.com
172.16.2.3      vbardolino.vbrew.com  vbardolino
172.16.2.4      vchianti.vbrew.com    vchianti
```

Assim como ocorre com uma série de endereços IP, você deve, por vezes, utilizar um nome simbólico para números de rede, também. Há-
Portanto, o *hosts* arquivo tem um companheiro chamado */ Etc / networks* que mapeia nomes de rede para números de rede, e vice-
versa. Na Cervejaria Virtual, podemos instalar um *redes* arquivo como este:[30]

```
# / Etc / redes para a Cervejaria Virtual
brew-net      172.16.1.0
vinho-net     172.16.2.0
```

Interface de configuração para IP

Após configurar o hardware, como explicado no capítulo 4, *Configurando o Hardware Serial*, Você tem que fazer estes dispositivos conhecidos para o software de rede do kernel. Um par de comandos são usados para configurar a rede, interfaces de trabalho e inicializar a tabela de roteamento. Estas tarefas são normalmente realizadas a partir da inicialização de rede
script cada vez que você inicializar o sistema. As ferramentas básicas para este processo são chamados `ifconfig` (Onde "se" significa
de interface) e `rota`.

`ifconfig` é usado para fazer uma interface acessível para a camada de rede do kernel. Isso envolve a atribuição de um endereço IP e outros parâmetros, e ativação da interface, também conhecido como "educar" a interface. Ser ativo, aqui, significa que o kernel irá enviar e receber datagramas IP através da interface. O mais simples maneira de invocá-lo é com:

`ifconfig` *interface ip address*

Este comando atribui *Endereço IP* para *interface* e ativa. Todos os outros parâmetros estão definidas para valores padrão. Para exemplo, a máscara de rede padrão é derivado da classe de rede do endereço IP, como *255.255.0.0* para um endereço de classe B. `ifconfig` é descrito em detalhes na seção "All About ifconfig".

`rota` permite-lhe adicionar ou remover as rotas da tabela de roteamento do kernel. Ele pode ser invocado como:

`route [adicionar | del] [-net |-host]` *alvo* `[`*se*`]`

A *adicionar* e *del* argumentos para determinar se adicionar ou excluir o caminho para *alvo*. A *-Net* e *-Host* argumentos dizer o comando se o destino é uma rede ou um host (um host é assumido se você não especificar). A *se*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

30 Observe que os nomes em *redes* não deve colidir com nomes dos *hosts* arquivo, ou então, alguns programas podem produzir resultados estranhos.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

argumento é novamente opcional e permite que você especifique a interface de rede que o percurso deve ser dirigida - o kernel do Linux faz uma suposição razoável se você não fornecer essa informação. Este tópico vai ser explicado em detalhes em sucessivas seções.

A interface de loopback

A interface primeiro a ser ativado é a interface loopback:

```
# ifconfig lo 127.0.0.1
```

Ocasionalmente, você vai ver o nome do host do manequim *localhost* sendo usado em vez do endereço IP. `ifconfig` vai procurar o nome na *hosts* arquivo, onde uma entrada deve declará-lo como o nome da máquina para *127.0.0.1*:

```
# Exemplo de / etc / hosts para a entrada localhost
localhost     127.0.0.1
```

Para visualizar a configuração de uma interface, você invocar `ifconfig`, Dando-lhe apenas o nome da interface como argumento:

```
$ ifconfig lo
eis       Encapsulamento do Link: Loopback Local
          inet addr: 127.0.0.1 Mask: 255.0.0.0
          UP RUNNING LOOPBACK  MTU: 3924 Métrica: 1
          pacotes RX: 0 erros: 0 descartados: 0 excesso: 0 quadro: 0
          Pacotes TX: 0 erros: 0 descartados: 0 excesso: 0 portadora: 0
          Colisões: 0
```

Como você pode ver, a interface loopback tenha sido atribuída uma máscara de *255.0.0.0*, Uma vez que *127.0.0.1* é uma classe

A
endereço.

Agora, você quase pode começar a brincar com o seu mini-rede. O que ainda falta é uma entrada na tabela de roteamento IP que informa que ele pode usar essa interface como rota para o destino *127.0.0.1*. Isso é feito usando-se:

```
# Route add 127.0.0.1
```

Novamente, você pode usar *localhost* em vez do endereço IP, desde que você inseriu-lo em seu */ Etc / hosts*.

Em seguida, você deve verificar se tudo funciona bem, por exemplo, utilizando `ping`.`ping` é o equiva-rede emprestado de um dispositivo de sonar.[31] O comando é usado para verificar se um determinado endereço é realmente acessível, e para medir
o atraso que ocorre quando você envia um datagrama para ele e vice-versa. O tempo necessário para esse processo é muitas vezes
referido como o "tempo de ida e volta":

```
# ping localhost
PING localhost (127.0.0.1): 56 bytes de dados
64 bytes from 127.0.0.1: icmp_seq = 0 ttl = 255 tempo = 0,4 ms
64 bytes from 127.0.0.1: icmp_seq = 1 ttl = 255 tempo = 0,4 ms
64 bytes from 127.0.0.1: icmp_seq = 2 ttl = 255 tempo = 0,4 ms
C ^
--- --- Localhost ping estatísticas
3 pacotes transmitidos, 3 packets received, 0% packet loss
ida e volta min / avg / max = 0.4/0.4/0.4 ms
#
```

Quando você invocar `ping` como mostrado aqui, ele continuará emitindo pacotes para sempre, a menos que interrompido pelo usuário.
A `C ^` marca o lugar onde nós pressionado Ctrl-C.

O exemplo anterior mostra que os pacotes de *127.0.0.1* sejam devidamente entregues e uma resposta é devolvida ao `ping` quase que instantaneamente. Isso mostra que você configurou com êxito a sua primeira interface de rede.

Se a saída você começa a partir `ping` não se assemelha ao indicado no exemplo anterior, você está em apuros. ~~Verifique todos os erros que indicam~~ que algum arquivo não foi instalado corretamente. Verifique se o `ifconfig` e `rota` binários que você usa são compatíveis com a versão do kernel você corre, e acima de tudo, que o kernel tenha sido compilado com a rede habilitada (você vê isso a partir da presença do */ Proc / net* diretório). Se você receber um erro

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

31 Alguém se lembra do Pink Floyd, "Echoes"?

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

mensagem dizendo "Rede inacessível", você provavelmente tem a `rota` comando errado. Certifique-se de usar o mesmo endereço que você deu a `ifconfig`.

Os passos descritos anteriormente são suficientes para usar aplicações de rede em uma máquina independente. Após adicionar o linhas mencionadas anteriormente ao seu script de inicialização de rede e ter certeza que ele será executado em tempo de boot, você pode reiniciar a máquina e experimentar várias aplicações. Por exemplo, `telnet localhost` deve estabelecer um`telnet` conexão com o seu anfitrião, dando-lhe uma `login:` prompt.

No entanto, a interface de loopback é útil não só como um exemplo em livros networking, ou como um banco de ensaio durante desenvolvimento, mas na verdade é usado por alguns aplicativos durante a operação normal.[32] Portanto, você sempre tem que configurá-lo, independentemente de sua máquina esteja conectada a uma rede ou não.

Interfaces Ethernet

Configurando uma interface Ethernet é praticamente a mesma que a interface de loopback, que apenas requer um pouco mais parâmetros quando você estiver usando sub-redes.

Na Cervejaria Virtual, temos a sub-rede IP, que foi originalmente uma rede de classe B, na classe C sub-redes. Para fazer a interface reconhecer isso, o `ifconfig` encantamento ficaria assim:

```
# ifconfig eth0 netmask 255.255.255.0 vstout
```

Este comando atribui a *eth0* interface o endereço IP do *vstout* (*172.16.1.2*). Se omitida, a máscara de rede, `se-config` poderia deduzir a máscara da classe de rede IP, o que resultaria em uma máscara incorreta de *255.255.0.0*. Agora, uma rápida mostra de seleção:

```
# ifconfig eth0
eth0      Link encap 10Mps Ethernet Endereço de HW  00:00: C0: 90: B3: 42
          inet addr Bcast 172.16.1.2 172.16.1.255 Máscara 255.255.255.0
          UP BROADCAST RUNNING  MTU 1500  Métrica 1
          pacotes RX 0 erros 0 descartados 0 0 superação
          Pacotes TX 0 erros 0 descartados 0 0 superação
```

Você pode ver que `ifconfig` ajusta automaticamente o endereço de broadcast (o *Bcast* campo) para o valor normal, que é o número do host de rede com todos os bits de host definido. Além disso, a unidade máxima de transmissão (o tamanho máximo
de datagramas IP que o kernel irá gerar para esta interface) foi definido para o tamanho máximo dos pacotes Ethernet:
1.500 bytes. Os padrões são geralmente o que você vai usar, mas todos esses valores podem ser overidden se necessário, com opções especiais, que serão descritos em "All About ifconfig".

Assim como para a interface loopback, agora você tem que instalar uma entrada de roteamento que informa o kernel sobre o net-trabalho que pode ser alcançado através *eth0*. Para a cervejaria virtual, você pode invocar `rota` como:

```
# rota add-net 172.16.1.0
```

No começo isso parece um pouco de magia, como, porque não é muito claro como `rota` detecta qual a interface a rota completamente. No entanto, o truque é bastante simples: o kernel verifica todas as interfaces que foram configurados até ao momento e
compara o endereço de destino (*172.16.1.0* neste caso) para a parte de rede do endereço de interface (isto é, o AND bit a bit do endereço da interface ea máscara de rede). A única interface que corresponde é *eth0*.

Agora, o que *-Net* opção para? Isto é usado porque `rota` pode lidar com ambas as rotas para as redes e vias de acesso hosts individuais (como você viu antes, com *localhost*). Quando um determinado endereço em notação decimal com pontos, `rota` tentativas
para adivinhar se é uma rede ou um nome, olhando os bits parte de host. Se parte do endereço de host é zero, `rota` assume que denota uma rede, caso contrário, `rota` toma-a como um endereço de host. Por isso, `rota` seria acho que *172.16.1.0* é um endereço de host em vez de um número de rede, porque ele não pode saber que nós usamos sub-ting. Nós temos que dizer `rota` explicitamente que denota uma rede, por isso, dar-lhe o *-Net* pavilhão.

É claro que o `rota` comando é um pouco entediante, tipo e é propenso a erros de ortografia. A mais conveniente abordagem é usar os nomes de rede foram definidos em */ Etc / networks*. Essa abordagem faz com que o comando muito mais legível, mesmo os *-Net* bandeira pode ser omitido porque `rota` sabe que *172.16.1.0* denota uma rede:

```
# route add-net brew
```

32 Por exemplo, todos os aplicativos baseados em RPC uso da interface loopback para registrar-se com a `portmapper` daemon at inicialização. Estas aplicações incluem NIS e NFS.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Agora que você terminou os passos de configuração básica, queremos ter certeza de que sua interface Ethernet é
realmente correndo alegremente. Escolha um host de sua rede Ethernet, por exemplo *vlager*, Digite e:

```
# ping vlager
vlager PING: pacotes de 64 bytes
64 bytes de 172.16.1.1: icmp_seq = 0. tempo = 11. ms
64 bytes de 172.16.1.1: icmp_seq = 1. tempo = 7. ms
64 bytes de 172.16.1.1: icmp_seq = 2. tempo = 12. ms
64 bytes de 172.16.1.1: icmp_seq = 3. tempo = 3. ms
C ^
---- Vstout. Vbrew.com PING Estatísticas ----
4 pacotes transmitidos, 4 pacotes recebidos, 0
de ida e volta (ms)     min / avg / max = 3/8/12
```

Se você não vir uma saída similar, algo está quebrado. Se você encontrar as taxas de perda anormal de pacotes, este aponta para um
problema de hardware, como terminadores incorreto ou ausente. Se você não receber qualquer resposta em tudo, você deve verificar o
configuração da interface com `netstat` descrito mais adiante "O Comando netstat". As estatísticas do pacote apresentado por `ifconfig` deve dizer se todos os pacotes foram enviados na interface em tudo. Se você tiver acesso
para o host remoto também, você deve ir para essa máquina e verificar as estatísticas da interface. Desta forma, você pode determinar exatamente onde os pacotes caiu. Além disso, você deve exibir as informações de roteamento com `rota` para ver se ambos os anfitriões têm a entrada correta de roteamento. `rota` imprime o kernel completo da tabela de roteamento
Quando chamado sem argumentos (*-N* apenas torna imprimir endereços, pontilhada quad ao invés de usar o host nome):

```
# route-n
Kernel tabela de roteamento
Destino      Gateway  Genmask         Flags Metric Ref Use    Iface
127.0.0.1    *        255.255.255.255 UH    1      0      112 eis
172.16.1.0   *        255.255.255.0   U     1      0       10 eth0
```

O significado detalhada desses campos é explicado mais tarde em "O Comando netstat". A *Bandeiras* coluna contém um lista de sinalizadores fixados para cada interface. *U* é sempre definido para as interfaces ativas, e *H* diz que o endereço de destino de-
observa um host. Se o *H* sinalizador é definido para uma rota que pretendia ser uma rota de rede, você tem que refazer a `rota` comando com a *-Net* opção. Para verificar se uma rota que você digitou é usado em tudo, verifique se o *Use* campo na segunda coluna aumenta para durar entre duas invocações de `ping`.

Roteamento através de um gateway

Na seção anterior, que abrangeu apenas o caso da criação de um host em uma única porta. Muito freqüentemente,
No entanto, encontra-redes conectadas entre si por gateways. Estes gateways podem simplesmente ligar dois Ethernets ou mais, mas também pode fornecer um link para o mundo exterior, como a Internet. Em ordem para usar uma porta-
Assim, você tem que fornecer informações de roteamento adicionais para a camada de rede.

O Ethernets da Cervejaria Virtual e da adega virtuais são ligadas através de um gateway tais, ou seja, o anfitrião *vlager*. Assumindo que *vlager* já foi configurado, só tem que adicionar outra entrada para *vstout*As rotas
tabela que informa o kernel que pode atingir todos os hosts da rede, através da Vinícola *vlager*. O Incanta apro-
ção de `rota` é mostrado abaixo, o *gw* palavra-chave que diz que o próximo argumento denota um gateway:

```
# route add gw vlager vinho-net
```

É claro que qualquer host na rede Winery quiser falar deve ter uma entrada de encaminhamento para a cervejaria da net-
de trabalho. Caso contrário, você só seria capaz de enviar dados para a rede Adega da rede cervejaria, mas a hosts na Adega seria incapaz de responder.

Este exemplo descreve apenas uma porta de entrada que alterna entre dois pacotes Ethernets isolado. Agora vamos supor que *vlager* também tem uma ligação à Internet (por exemplo, através de uma ligação SLIP adicional). Em seguida, gostaríamos de dados
gramas para *qualquer* rede de destino diferente da cervejaria para ser entregue ao *vlager*. Esta ação pode ser acom-
te executados, tornando-o gateway padrão para *vstout*:

```
# route add default gw vlager
```

O nome da rede *padrão* é uma abreviação para *0.0.0.0*, O que denota a rota padrão. A rota padrão encontrados

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

cada destino e será utilizada se não houver uma rota mais específica que corresponda. Você não tem que adicionar este nome para */ Etc / networks* porque ele é construído em `rota`.

Se você ver as taxas de perda de pacotes em alta quando pingar um host por trás de uma ou mais portas, isso pode sugerir uma grande con-
rede sugerido. A perda de pacotes não é tanto devido a deficiências técnicas quanto ao excesso de cargas temporárias para-hosts piedade, que os faz atrasar ou mesmo queda de datagramas de entrada.

Configurando um Gateway

Configurando uma máquina para trocar pacotes entre duas redes Ethernet é bastante simples. Suponha que estamos de volta na *vlager*, Que está equipado com duas placas Ethernet, cada um conectado a uma das duas redes. Tudo que você precisa fazer é configurar as duas interfaces em separado, dando-lhes os respectivos endereços IP e rotas correspondentes, e É isso aí.

É bastante útil para adicionar informações sobre as duas interfaces para o *hosts* arquivo, como mostrado no exemplo a seguir, de forma
temos nomes acessível para eles, também:

```
172.16.1.1      vlager.vbrew.com    vlager vlager-if1
172.16.2.1      vlager-if2
```

A seqüência de comandos para configurar as duas interfaces é então:

```
# ifconfig eth0-vlager if1
# route add-net brew
# ifconfig eth1 vlager-if2
# route add-net vinho
```

Se esta seqüência não funciona, verifique se o kernel foi compilado com suporte para o encaminhamento de IP ativado. Uma boa maneira de fazer isso é garantir que o primeiro número na segunda linha de */ Proc / snmp / net* é definido como `1`.

A Interface PLIP

Uma ligação PLIP usado para conectar dois computadores é um pouco diferente de uma rede Ethernet. PLIP links são um exemplo de
que são chamados *ponto-a-ponto* links, o que significa que há uma única máquina em cada extremidade da ligação. Redes como a
Ethernet são chamados *transmissão* redes. Configuração de enlaces ponto-a-ponto é diferente porque, ao contrário ampla redes elenco, links ponto-a-ponto de não suportar uma rede própria.

PLIP fornece links muito barato e portátil entre computadores. Como exemplo, vamos considerar o laptop com-
putador de um funcionário na Cervejaria Virtual que está conectado ao *vlager* via PLIP. O portátil em si é chamada *vLite* e tem apenas uma porta paralela. Na altura do arranque, esta porta será registrado como *plip1*. Para ativar o link, você tem que configurar o *plip1* interface utilizando os seguintes comandos:[33]

```
# ifconfig plip1 vlager pointopoint vLite
# route add default gw vlager
```

O primeiro comando configura a interface, dizendo que o kernel que esta é uma ligação ponto a ponto, com o controle remoto lado que tem o endereço do *vlager*. A segunda instala a rota padrão, utilizando *vlager* como gateway. Em *vlager*, Um semelhantes `ifconfig` comando é necessário para ativar o link (a `rota` invocação não é necessário):

```
# ifconfig plip1 vLite pointopoint vlager
```

Note-se que o *plip1* interface em *vlager* não precisa de um endereço IP separado, mas pode também ser dado o endereço *172.16.1.1*. Redes Point-to-point não suporte uma rede diretamente, de modo a interfaces não precisam de um endereço na qualquer rede de suporte. O kernel usa as informações da interface na tabela de roteamento para evitar qualquer possível con-fusão.[34]

Agora nós configuramos o roteamento do laptop à rede da cervejaria, o que ainda está faltando é uma forma de percurso de qualquer um dos anfitriões da cervejaria para *vLite*. Uma forma particularmente embaraçoso é para adicionar uma rota específica para cada
tabela de roteamento do host que os nomes *vlager* como um gateway para *vLite*:

```
# route add gw vlager vLite
```

O roteamento dinâmico oferece uma opção muito melhor para as rotas temporária. Você pode usar `gated`, Um daemon de roteamento,
que você teria que instalar em cada máquina da rede para distribuir informações de roteamento dinamicamente.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

camente. A opção mais fácil, no entanto, é a utilização de *ARP* (Address Resolution Protocol). Com proxy ARP, *vlager*

33 Note-se que pointopoint não é um erro de digitação. É realmente escrito como este.

34 Por uma questão de precaução, você deve configurar uma ligação PLIP ou SLIP somente depois que você configurar completamente as entradas de tabela de roteamento para o seu

Ethernets. Com alguns kernels mais antigos, o seu percurso de rede, de outra forma acabam apontando para a ligação ponto a ponto.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

responde a qualquer consulta ARP para *vLite* enviando o seu próprio endereço Ethernet. Todos os pacotes para *vLite* vai acabar em
vlager, Que depois encaminha para o laptop. Voltaremos a proxy ARP na seção "Verificar a
Tabelas ARP ".

Atual *net-tools* versões contêm uma ferramenta chamada `plipconfig`, Que permite que você defina pa timing certo PLIP-tros. O IRQ a ser usado para a porta da impressora pode ser configurada usando o `ifconfig` comando.

As interfaces SLIP e PPP

Embora as ligações SLIP e PPP são apenas simples ligações ponto-a-ponto como conexões PLIP, há muito mais para ser dito sobre eles. Normalmente, o estabelecimento de uma conexão SLIP implica a marcação de um site remoto através de seu mo-
dem e definindo a linha de série para o modo de SLIP. PPP é utilizado de forma semelhante. Discutimos SLIP e PPP em detalhe no capítulo 7 eo capítulo 8, *O protocolo ponto-a-Ponto*.

A interface dummy

A interface do boneco é um pouco exótico, mas bastante útil, no entanto. Seu principal benefício é com hosts autônomos e máquinas cuja única conexão de rede IP é uma ligação dial-up. Na verdade, estes últimos são a maioria dos hosts autônomos o tempo também.

O dilema com hosts autônomos é que eles só têm um único dispositivo de rede ativo, o dispositivo de loopback, que geralmente é atribuído o endereço *127.0.0.1*. Em algumas ocasiões, entretanto, você deve enviar dados para o "oficial-cial "endereço IP do host local. Por exemplo, considere o laptop *vLite*, Que foi desligado de uma rede durante a vigência deste exemplo. Um aplicativo em *vLite* pode agora querer enviar dados para outro aplicativo no mesmo hospedeiro. Olhando para cima *vLite* em */ Etc / hosts* gera um endereço IP *172.16.1.65*, Para que o aplicativo tenta enviar para o
este endereço. Como a interface loopback é atualmente a única interface ativa na máquina, o kernel não tem idéia de que *172.16.1.65* na verdade se refere a si mesmo! Consequentemente, o kernel descarta o datagrama e retorna um erro para o aplicativo.

Isto é onde as etapas do dispositivo simulado pol resolve o dilema simplesmente servir como o alter ego do circuito volta interface. No caso da *vLite*, Basta dar-lhe o endereço *172.16.1.65* e adicionar uma rota de host apontando para ele. Cada datagrama para *172.16.1.65* é então entregue localmente. A invocação apropriada é:[35]

```
#vLite ifconfig dummy
#route add vLite
```

IP Alias

miolo novo suporte um recurso que pode substituir completamente a interface dummy e servir outras funções úteis. *IP Alias* permite configurar vários endereços IP para um dispositivo físico. No caso mais simples, você pode replicar a função da interface dummy, configurando o endereço do host como um alias para o loopback inter-rosto e evitar completamente usando a interface do manequim. Nos usos mais complexos, você pode configurar sua máquina para
parecido com muitos hosts diferentes, cada um com seu próprio endereço IP. Essa configuração é às vezes chamado de "Virtual Hospedagem ", embora tecnicamente ele também é usado para uma variedade de outras técnicas.[36]

Para configurar um apelido para uma interface, você deve primeiro assegurar que o seu kernel foi compilado com suporte para Alias IP (verifique se você tem um */ Proc / net / ip_alias* arquivo, se não, você terá que recompilar o kernel). Configuração de um IP alias é praticamente idêntica à configuração de um dispositivo de rede real, você usa um nome especial para
indicar que é um apelido que você deseja. Por exemplo:

```
# ifconfig lo: 0 172.16.1.1
```

Este comando deve produzir um alias para a interface de loopback com o endereço `172.16.1.1`. aliases IP são referidas, acrescentando:*n* ao dispositivo de rede atual, em que "n" é um inteiro. No nosso exemplo, a rede

35 O dispositivo é chamado de dummy *dummy0* Se ele é carregado como um módulo ao invés de escolhê-lo como uma opção do kernel embutido. Isto é ser-
Porque você é capaz de carregar vários módulos e tem mais de um dispositivo de manequim.
36 Mais corretamente, usando o IP aliasing é conhecida como camada de rede virtual de hospedagem. É mais comum na WWW e mundos STMP usar

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

camada de aplicativo de hospedagem virtual, no qual o mesmo endereço IP é usado para cada host virtual, mas um nome diferente é transmitido a cada SOLICITAÇÃO camada. Serviços como FTP não são capazes de operar desta maneira, e eles exigem a camada de rede virtual de hospedagem.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

dispositivo que estamos criando o alias é sobre `eis`, E estamos criando um alias numerados de zero para ele. Desta forma, um único
dispositivo físico pode suportar um número de pseudônimos.

Cada alias pode ser tratado como se fosse um dispositivo separado, e na medida em que o kernel do software IP está em causa, Será, no entanto, ele estará compartilhando o seu hardware com outra interface.

Tudo Sobre ifconfig

Há muitos parâmetros mais `ifconfig` que temos descrito até agora. A sua invocação normal é este:

`ifconfig` *interface* `[`*endereço* `[`*parâmetros*`]]`

interface é o nome da interface, e *endereço* é o endereço IP a ser atribuído à interface. Este tanto pode ser um endereço IP na notação "dotted quad ou um nome que `ifconfig` vai procurar em */ Etc / hosts*.

Se `ifconfig` é invocado com apenas o nome da interface, ele exibe configuração que interface. Quando invocado sem parâmetros, ele exibe todas as interfaces que você configurou, até agora, um *-Um* opção forças para mostrar a os inativos também. A invocação de exemplo para a interface Ethernet *eth0* pode ser parecido com este:

```
# ifconfig eth0
eth0      Link encap 10 Mbps Ethernet HWaddr 00:00: C0: 90: B3: 42
          inet addr Bcast 172.16.1.2 172.16.1.255 Máscara 255.255.255.0
          UP BROADCAST RUNNING  MTU 1500  Metric 0
          pacotes RX 3136 erros de 217 caiu 7 superação 26
          Pacotes TX 1752 erros caiu 25 0 0 superação
```

A `MTU` e `Métrica` campos mostram a MTU atual e valor da métrica para essa interface. O valor da métrica é tradicionalmente utilizados por alguns sistemas operacionais para calcular o custo de uma rota. Linux não utiliza este valor ainda, mas
define a compatibilidade, no entanto.

A `RX` e `TX` linhas mostram quantos pacotes foram recebidos ou transmitidos sem erros, os erros de quantas ocorreram, quantos pacotes foram descartados (provavelmente por causa da pouca memória), e quantos foram perdidos devido de superação. derrapagens receptor geralmente ocorrem quando vêm em pacotes mais rápido do que o kernel pode atender o último
interrupção. A bandeira valores impressos pela `ifconfig` correspondem, aproximadamente, aos nomes de suas opções de linha de comando;
que será explicado mais tarde.

A seguir está uma lista de parâmetros reconhecidos pelo `ifconfig` com os nomes bandeira correspondente. Opções que basta ligar um recurso também permite que ele seja desligado novamente precedendo o nome da opção por um traço (-).

`até`

Esta opção faz com que uma interface acessível para a camada IP. Esta opção está implícita quando um *endereço* é dado na linha de comando. Também pode ser usado para reativar um interface que tenha sido tomada para baixo tem-porariam ente com o `baixo` opção.

Esta opção corresponde ao pavilhão *UP* e *RUNNING*.

`baixo`

Esta opção representa um interface inacessível para a camada IP. Isso efetivamente desativa todo o tráfego IP através da interface. Note que esta opção também serão automaticamente excluir todas as entradas de roteamento que usam este
interface.

`netmask` *máscara*

Esta opção atribui uma máscara para ser utilizado pela interface. Ela pode ser dada através hexa de 32 bits-número decimal precedido por 0x ou como dotted quad de números decimais. Embora o formato dotted quad é mais comum, a representação hexadecimal é mais fácil trabalhar com ele. Netmasks são essencialmente binários, e é mais fácil fazer binário-para-hexadecimal de conversão binário para decimal.

`pointopoint` *endereço*

Esta opção é usada para links IP ponto-a-ponto que envolvem apenas dois hosts. Esta opção é necessária para con-Figura interfaces SLIP ou PLIP, por exemplo. Se um endereço ponto-a-ponto foi definido, `ifconfig` dis-desempenha o *Pointopoint* pavilhão.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`transmissão` *endereço*

O endereço de broadcast é feito geralmente a partir do número da rede, definindo todos os bits da parte de host.
Algumas implementações do IP (sistemas derivados do BSD 4.2, por exemplo) usam um esquema diferente, na qual todos os bits parte de host estão habilitados em seu lugar. A *transmissão* opção se adapta a estes ambientes estranhos. Se um
`irq` endereço de broadcast tiver sido definida, `ifconfig` exibe o *BROADCAST* pavilhão.

Esta opção permite que você defina a linha de IRQ usado por certos dispositivos. Isto é especialmente útil para PLIP, mas também pode ser útil para determinadas placas Ethernet.

`métricas` *número*

Esta opção pode ser usada para atribuir um valor métrico para a entrada da tabela de roteamento criado para a interface.

Este
métrica é usada pelo Routing Information Protocol (RIP) para construir tabelas de roteamento para a rede.[37] The métrica padrão utilizado por `ifconfig` é zero. Se você não executar um daemon RIP, você não necessita esta opção por
todos, se você fizer isso, você raramente vai precisar alterar o valor da métrica.

`mtu` *bytes*

Isso define a unidade máxima de transmissão, que é o número máximo de octetos a interface é capaz
para tratar de uma transação. Para Ethernet, os padrões de MTU para 1500 (o maior tamanho permitido de um Pacote Ethernet); para interfaces SLIP, é 296. (Não há nenhuma restrição sobre a MTU de ligações SLIP, o que valor é um bom compromisso.)

`arp`

Esta é uma opção específica de transmissão de redes como Ethernets ou packet radio. Ele permite o uso de
o Address Resolution Protocol (ARP) para detectar os endereços físicos dos hosts ligados à rede-
de trabalho. Quanto às redes de transmissão, é ativado por padrão. Se ARP está desativado, `ifconfig` exibe o *NOARP*
pavilhão.

`Arp`

Esta opção desativa o uso do ARP sobre esta interface.

`promisc`

Esta opção coloca a interface em modo promíscuo. Em uma rede de transmissão, o que torna a interface
receber todos os pacotes, independentemente de que estavam destinados para este host ou não. Esta rede permite análise de tráfego usando filtros de pacotes e tal, também chamado *Ethernet snooping*. Normalmente, esta é uma boa tecnologia,
nique para caçar problemas de rede que são de outra maneira difícil de detectar. Ferramentas como `tcpdump` confiar nisso.

Por outro lado, esta opção permite que os atacantes para fazer coisas desagradáveis, tais como a nata do tráfego de sua rede para senhas. Você pode proteger contra este tipo de ataque, que proíbe qualquer pessoa de conectar seus computadores para sua Ethernet. Você também pode usar protocolos de autenticação segura, como Kerberos ou o login shell seguro suite.[38] Esta opção corresponde à *PROMISC* pavilhão.

`-Promisc`

Esta opção ativa o modo promíscuo fora.

`allmulti`

endereços Multicast são como endereços de broadcast Ethernet, exceto que em vez de automaticamente, incluindo todo mundo, as únicas pessoas que recebem pacotes enviados a um endereço multicast são aqueles programados para lis-
dez para ele. Isso é útil para aplicações como videoconferência baseados em Ethernet e áudio de rede, para que apenas os interessados podem ouvir. Endereçamento multicast é suportado pela maioria, mas não todos, Ethernet drivers. Quando esta opção for ativada, a interface recebe e transmite os pacotes multicast para processamento. Esta opção corresponde à *ALLMULTI* pavilhão.

`-Allmulti`

Esta opção transforma endereços multicast fora.

[37] RIP escolhe a melhor rota para um determinado host com base na "extensão" do caminho. Ele é calculado somando-se a métrica individual

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Os valores de cada elo de host para host. Por padrão, um hop tem comprimento 1, mas pode ser qualquer inteiro positivo menor que 16. (A duração da rota é de 16
igual ao infinito. Essas rotas são consideradas inutilizáveis.) A *métricas* parâmetro define esse custo hop, que é então transmitido pelo roteamento daemon.

38 ssh podem ser obtidas *ftp.cs.hut.fi* em */ Pub / ssh*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O comando netstat

`netstat` é uma ferramenta útil para verificar sua configuração de rede e atividade. É na verdade uma coleção de diver-
ferramentas eral agrupados. Discutimos cada uma das suas funções nas seções a seguir.

Exibindo a tabela de roteamento

Quando você invocar `netstat` com o *-R* bandeira, que exibe a tabela de roteamento do kernel no modo como temos vindo a

fazer
com `rota`. Em *vstout*, Que produz:

```
# netstat-nr
Kernel tabela de roteamento IP
Destino       Gateway      Genmask         Bandeiras          MSS Janela Iface irtt
127.0.0.1     *            255.255.255.255 UH       0 0          0 eis
172.16.1.0    *            255.255.255.0   U        0 0          0 eth0
172.16.2.0    172.16.1.1   255.255.255.0   UG       0 0          0 eth0
```

A *-N* opção faz com que `netstat` imprimir endereços como números pontilhados quad IP em vez de o anfitrião simbólico e
Os nomes de rede. Esta opção é especialmente útil quando você quiser evitar lookups endereço na rede (por exemplo,
a um servidor de DNS ou NIS).

A segunda coluna da `netstat`'Mostra a saída do portão de entrada para que os pontos de entrada de roteamento. Se nenhum

gateway é
usado, um asterisco é mostrado. A terceira coluna mostra a "generalidade" da rota, ou seja, a máscara de rede
para esta rota. Quando um determinado endereço IP para encontrar um caminho adequado para o kernel através de cada etapas do encaminhamento
entradas da tabela, tendo a operação AND do endereço e do genmask antes de compará-lo ao destino da
percurso.

A quarta coluna exibe os seguintes sinalizadores que descrevem o percurso:

`G`

A rota usa um gateway.

`U`

A interface a ser utilizada está acima.

`H`

Apenas um único hospedeiro pode ser alcançada através da rota. Por exemplo, este é o caso para a entrada de loopback *127.0.0.1*.

`D`

Esta rota é criada dinamicamente. Ele é definido se a entrada de tabela foi gerada por um daemon de roteamento como `gated` ou por uma mensagem de redirecionamento ICMP (ver "O Internet Control Message Protocol" no Capítulo 2).

`M`

Este percurso está definido se a entrada de tabela foi modificado por uma mensagem de redirecionamento ICMP.

`!`

A rota é uma rota rejeitada e datagramas serão descartados.

As próximas três colunas mostram o MSS, Janela e irtt que será aplicado para conexões TCP estabelecida através de
esta rota. O MSS é o tamanho máximo do segmento e é o tamanho do maior datagrama o kernel irá con-
estrutura para a transmissão por esta via. A Janela é a quantidade máxima de dados o sistema irá aceitar em um
único estouro de um host remoto. O acrônimo `irtt` significa "tempo inicial de ida e volta." O protocolo TCP en-
Sures que os dados sejam entregues de forma confiável entre hosts através da retransmissão de um datagrama se ele foi perdido. O TCP pro-
tocolo mantém uma contagem de quanto tempo leva para um datagrama a ser entregue até o final remoto, e uma ac-
e Conhecimento a ser recebido para que ele saiba quanto tempo a aguardar antes de assumir um datagrama precisa retrans-
mitido, este processo é chamado de tempo de ida e volta. O tempo de ida e volta inicial é o valor que o protocolo TCP
usará quando uma conexão é estabelecida pela primeira vez. Para a maioria dos tipos de rede, o valor padrão é bom, mas para alguns
redes lentas, nomeadamente certos tipos de redes de rádio amador em pacotes, o tempo é curto demais e faz com que desneces-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

retransmissão necessárias. A `irtt` valor pode ser definido usando o `rota` comando. Valores de zero nestes campos médios que o padrão está sendo usado.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Finalmente, o último campo exibe a interface de rede que irá usar esta rota.

Resultados de estatísticas da interface

Quando chamado com a *-I* bandeira, `netstat` exibe estatísticas para as interfaces de rede configuradas. Se o *-Um* opção também é dado, imprime *todos* interfaces presentes no kernel, e não apenas aqueles que tenham sido configuradas atualmente. Em *vstout*, A saída do `netstat` será parecido com este:

```
# netstat-i
Kernel tabela Interface
Iface MTU Met  RX-RX-ERR OK DRP RX-RX-OVR  TX-TX-ERR OK Bandeiras DRP TX-TX-OVR
eis     0   0   3185      0      0      0   3185      0      0      0 BLRU
eth0 1500   0 972633     17     20    120 628711    217      0      0 BRU
```

A `MTU` e `Met` campos mostram os valores de MTU atual e métricas para essa interface. A `RX` e `TX` colunas mostrar quantos pacotes foram recebidos ou transmitidos sem erros (`RX-OK`/`TX-OK`) Ou danificados (`RX-ERR`/`TX-ERR`), Quantos foram descartados (`RX-DRP`/`DRP-TX`), E quantos foram perdidos por causa de uma superação (`RX-OVR`/`TX-OVR`).

A última coluna mostra os sinalizadores que foram definidos para esta interface. Estes personagens são versões de um caracter dos nomes bandeira longos que são impressas quando você mostrar a configuração da interface com `ifconfig`:

`B`

Um endereço de broadcast foi definido.

`L`

Esta interface é um dispositivo de loopback.

`M`

Todos os pacotes são recebidos (modo promíscuo).

`O`

ARP é desligado para esta interface.

`P`

Esta é uma conexão ponto-a-ponto.

`R`

Interface está rodando.

`U`

Interface é para cima.

Resultados de conexões

`netstat` suporta um conjunto de opções para exibir soquetes ativa ou passiva. As opções *T*,*-U*,*-W*E *-X* show ativa TCP, UDP, RAW, ou conexões socket Unix. Se você fornecer o *-Um* bandeira, além disso, sockets que são de esperar ção de uma conexão (ou seja, músicas) são exibidos também. Esta exposição vai lhe dar uma lista de todos os servidores que estão
atualmente em execução no sistema.

Invocar `netstat-ta` em *vlager* produz esta saída:

```
$ netstat-ta
Internet conexões ativas
Proto Recv-Q Send-Q Endereço Local   Foreign Address    (Estado)
tcp        0      0 *: domínio      : *                OUÇA
tcp        0      0 *: tempo        : *                OUÇA
tcp        0      0 *: smtp         : *                OUÇA
tcp        0      0 vlager: smtp    vstout: 1040       ESTABLISHED
tcp        0      0 *: telnet       : *                OUÇA
tcp        0      0 localhost: 1046 vbardolino: telnet ESTABLISHED
tcp        0      0 *: chargen      : *                OUÇA
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
tcp        0      0 *: diurna           : *               OUÇA
tcp        0      0 *: descartar        : *               OUÇA
tcp        0      * 0: echo             : *               OUÇA
tcp        0      0 *: shell            : *               OUÇA
tcp        0      0 *: login            : *               OUÇA
```

Este resultado mostra a maioria dos servidores simplesmente à espera de uma ligação recebida. No entanto, a quarta linha mostra um
conexão de SMTP de entrada *vstout*Ea sexta linha diz que há uma saída `telnet` conexão com *vbardolino*.[39]

Usando o *-Um* bandeira, por si só irá exibir todos os soquetes de todas as famílias.

Verificando as tabelas ARP

Em algumas ocasiões, é útil para visualizar ou alterar o conteúdo das tabelas ARP do kernel, por exemplo, quando você suspeitar de um duplicado endereço na Internet é a causa de algum problema de rede intermitente. A `arp` ferramenta foi feita para situações como esta. Suas opções de linha de comando são:

```
arp [v] [-t  hwtype]-A [hostname]
arp [v] [-t  hwtype]-S    hwaddr hostname
arp [v]-d   hostname   [hostname...]
```

Todos *hostname* argumentos podem ser tanto simbólico hostnames ou endereços IP na notação "dotted quad.

A primeira invocação exibe a entrada ARP para o endereço IP ou o host especificado, ou todos os hosts sabe se não *host nome* é dado. Por exemplo, invocando `arp` em *vlager* pode produzir:

```
# arp-a
endereço IP     Tipo de HW             Endereço HW
172.16.1.3      10 Mbps Ethernet       00:00: C0: 5A: 42: C1
172.16.1.2      10 Mbps Ethernet       00:00: C0: 90: B3: 42
172.16.2.4      10 Mbps Ethernet       00:00: C0: AA: 04:69
```

que mostra o endereço de Ethernet *vlager*,*vstout* e *Vale*.

Você pode limitar a exibição para o tipo de hardware especificado usando o *T* opção. Isso pode ser *éter*,*ax25*Ou *ProNet*, permanente para Ethernet de 10 Mbps; AX.25 AMPR e IEEE 802,5 equipamentos token ring, respectivamente.

A *-S* opção é usada para adicionar de forma permanente *hostname*'S endereço Ethernet para as tabelas ARP. A *hwaddr* argumento especifica o endereço de hardware, que por padrão é esperado para ser um endereço Ethernet especificado como seis hexa-bytes decimais separados por vírgulas. Você também pode definir o endereço de hardware para outros tipos de hardware, usando o
T opção.

Por alguma razão, as consultas ARP para o host remoto às vezes falham, por exemplo, quando o seu condutor ARP é buggy ou há um outro host na rede que erroneamente se identifica com o endereço IP que de acolhimento; este problema requer que você adicionar manualmente um endereço IP na tabela ARP. endereços Hard-fiação IP na tabela ARP também é um (Muito drástico) medida para se proteger de hosts em sua rede Ethernet que se apresentam como uma outra pessoa.

Invocar `arp` usando o *-D* switch exclui todas as entradas ARP relativas ao acolhimento dado. Essa opção pode ser utilizada para força a interface a tentar re-obter o endereço Ethernet para o endereço IP em causa. Isso é útil quando um sistema de informação errada foi transmitida ARP errado (é claro, você tem que reconfigurar o partido primeiro hospedeiro).

A *-S* opção também pode ser usado para implementar *proxy* ARP. Esta é uma técnica especial através do qual um anfitrião, digamos
portão, Atua como um portal para outra máquina chamada *fnord* fingindo que os dois endereços referem-se ao mesmo host, ou seja, *portão*. Fá-lo através da publicação de uma entrada ARP para *fnord* que aponta para sua própria interface Ethernet. Agora
quando um host envia uma consulta ARP para *fnord*,*portão* retornará uma resposta contendo seu próprio endereço Ethernet. A host consulta irá enviar para todos os datagramas *portão*, Que respeitosamente os encaminha para *fnord*.

[39] Você pode dizer se a conexão está de saída do números de porta. O número da porta indicado para uma saída [illegible] é uma

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

inteiros simples. Sobre o host que está sendo chamado, uma porta de serviço bem conhecido estarão em uso para o qual `netstat` usa o nome simbólico, como `smtp`, Encontrada em */ Etc / services*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Estes contorções pode ser necessário quando você deseja acessar *fnord* de uma máquina DOS com um TCP

quebrado
implementação que não entende muito bem de roteamento. Quando você usa proxy ARP, ele será exibido para o DOS
máquina, como se *fnord* foi na sub-rede local, para que ele não precisa saber sobre como rota através de um gateway.

Outro aplicativo útil de proxy ARP é quando um dos seus anfitriões atua como porta de entrada para algum

outro host só
temporariamente, por exemplo, através de uma conexão dial-up. No exemplo anterior, encontramos o laptop *vLite*, Que foi conectado a *vlager* através de uma ligação PLIP de vez em quando. Naturalmente, esse aplicativo só funcionará se o endereço do host que você deseja fornecer proxy ARP para está na mesma sub-rede como o seu gateway. *vstout* poderia ARP proxy para qualquer máquina na subrede Brewery (*172.16.1.0*), Mas nunca para um host na subrede Winery (*172.16.2.0*).

A invocação apropriada para fornecer proxy ARP para *fnord* é apresentado a seguir, claro, o endereço Ethernet dada deve ser o de *portão*:

```
# Arp-s fnord 00:00: c0: a1: 42: e0 pub
```

A entrada ARP pode ser removido novamente invocando:

```
# Arp-d fnord
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 6 - Serviço de Nome e configuração do resolvedor

Como discutimos no Capítulo 2, *Problemas de rede TCP / IP*, A rede TCP / IP pode confiar nos regimes diferentes para converter nomes em endereços. A maneira mais simples é uma tabela de host armazenados em */ Etc / hosts*. Isso é útil apenas para
Pequenas redes locais que são executados por um único administrador e não têm outra tráfego IP, com o mundo exterior. A formato do *hosts* arquivo já foi descrito no Capítulo 5, *Configurando Redes TCP / IP*.

Alternativamente, você pode usar o *Berkeley Internet Name Domain serviço* (BIND) para resolver nomes de host para IP endereços. Configurando o BIND pode ser uma tarefa real, mas uma vez que você fez isso, você pode facilmente fazer alterações no
topologia de rede. No Linux, como em muitos outros sistemas Unixish, nome de serviço é fornecido através de um programa chamada `nomeado`. Na inicialização, ele carrega um conjunto de arquivos mestre em seu cache interno e espera para as consultas de controlo remoto ou
processos locais de usuário. Existem diferentes maneiras para configurar o BIND, e não exigem que você execute um servidor de nome
cada host.

Este capítulo pode fazer pouco mais do que dar um esboço de como o DNS funciona e como operar um servidor de nomes. É deve ser suficiente se você tem uma pequena rede local e um uplink Internet. Para obter as informações mais atuais, você pode querer verificar a documentação contida no pacote fonte do BIND, que fornece páginas de manual, a liberação notas, e os *Guia do Operador do BIND* (BOG). Não deixe que este nome te assusta, é realmente muito útil documento. Para uma cobertura mais abrangente do DNS e problemas associados, você pode encontrar *DNS e BIND* por Paulo Albitz e Cricket Liu (O'Reilly) uma referência útil. questões de DNS pode ser respondida em um newsgroup chamado comp.protocols.tcp-ip.domains. Para detalhes técnicos, o Domain Name System é definido por números RFC-bros 1033, 1034 e 1035.

A Biblioteca Resolver

O termo *resolvedor* não se refere a um pedido especial, mas para a biblioteca de resolução. Esta é uma coleção de funções que podem ser encontrados na biblioteca C padrão. As rotinas de central são *gethostbyname (2)* e *gethostbyaddr (2)*, que olhar para todos os endereços IP associados a um nome de anfitrião, e vice-versa. Eles podem ser configurados para simplesmente
procurar as informações em *hosts*, A consulta a um número de servidores de nome DNS, ou para usar o *hosts* banco de dados da Net
trabalho Information Service (NIS).

As funções de resolução de ler arquivos de configuração quando eles são chamados. A partir desses arquivos de configuração, que de-
minar quais bancos de dados para consulta, em que ordem, e outros detalhes pertinentes ao modo como você configurou seu ambien-
ente. A biblioteca padrão mais antigo do Linux, libc, usado */ Etc / host.conf* como o seu arquivo de configuração mestre, mas a versão 2
da biblioteca padrão GNU, glibc, usa */ Etc / nsswitch.conf*. Vamos descrever cada um em sua vez, já que ambos são comumente utilizado.

O host.conf Arquivo

A */ Etc / host.conf* informa o Linux mais antigas funções da biblioteca padrão de resolução de que os serviços de usar, e em que da ordem.

Opções na *host.conf* deve aparecer em linhas separadas. Os campos podem ser separados por espaço em branco (espaços ou tabulações). A
cerquilha (#) Apresenta um comentário que se estende até o fim da linha. As opções disponíveis são as seguintes:

fim

> Esta opção determina a ordem em que os serviços sejam julgados resolver. As opções válidas são *vincular* para consultar o nome do servidor, *hosts* para pesquisas em */ Etc / hosts*E *nis* para pesquisas de NIS. Qualquer ou todos eles pode ser especificado. A ordem em que aparecem na linha determina a ordem em que os res-
> olver serviços serão julgados.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

multi

`multi` toma *em* ou *fora* como opções. Isso determina se um hospedeiro */ Etc / hosts* é permitido ter vários IP endereços, que é normalmente referido como sendo "multi-homed". O padrão é off. Esta bandeira não tem efei- não tem efeito em consultas DNS ou NIS.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

nospoof

Como explicaremos na seção "Pesquisas Reversas", o DNS permite-lhe encontrar o nome da máquina pertencente à um endereço IP usando o *in-addr.arpa* domínio. As tentativas dos servidores de nome para indicar esse nome falso são chamados *spoofing*. Para se proteger, a resolução pode ser configurado para verificar se o original endereço IP é de fato associado ao hostname obtidos. Se não, o nome é rejeitada e um erro é devolvido. Este comportamento está ligado através da criação *nospoof* em.

alerta

Esta opção tem *em* ou *fora* como argumentos. Se ele estiver ligado, qualquer tentativa paródia fará com que o resolvedor de
log uma mensagem para o `syslog` facilidade.

aparar

Esta opção tem um argumento especificando um nome de domínio que será removido antes de hostnames pesquisa. Isso é útil para *hosts* entradas, para o qual você pode apenas querer especificar nomes de máquinas sem domínio local. Se você especificar o nome do domínio local aqui, ele será removido de uma pesquisa de um host com o nome de domínio local anexado, permitindo a pesquisa em */ Etc / hosts* para ter sucesso. O domínio nome que você adicionar deve terminar com o exemplo do personagem (, (.)`linux.org.au.`) Se `aparar` é para funcionar corretamente.

aparar opções de acumular, você pode considerar o seu acolhimento como local para vários domínios.

Um arquivo de exemplo para *vlager* é mostrado na Exemplo 6.1.

Exemplo 6.1: Exemplo host.conf Arquivo

```
# / Etc / host.conf
# Temos chamado a correr, mas não NIS (ainda)
fim     bind, hosts
# Permitir addrs múltiplas
multi   em
Guarda # contra as tentativas da paródia
nospoof em
# Trim domínio local (não é realmente necessário).
aparar  vbrew.com.
```

Resolver as variáveis de ambiente

As configurações da *host.conf* pode ser substituído com um número de variáveis de ambiente:

RESOLV_HOST_CONF

Esta variável especifica um arquivo para ser lido em vez de */ Etc / host.conf*.

RESOLV_SERV_ORDER

Essa variável substitui o *fim* opção prevista no *host.conf*. Serviços são dadas como *hosts*,*vincular*E *nis*, separados por um espaço, vírgula, dois pontos ou ponto e vírgula.

RESOLV_SPOOF_CHECK

Esta variável determina as medidas tomadas contra a falsificação. É completamente desativado por *fora*. O values *advertir* e *advertir fora* permitir a verificação da paródia girando logon e logoff, respectivamente. Um valor de * gira em torno de falsificar cheques, mas deixa o recurso de log, conforme definido no *host.conf*.

RESOLV_MULTI

Esta variável usa um valor de *em* ou *fora* para substituir o *multi* opções de *host.conf*.

RESOLV_OVERRIDE_TRIM_DOMAINS

Esta variável especifica uma lista de domínios da guarnição que se sobrepõem aos indicados no *host.conf*. Trim domínios foram
explicado anteriormente, quando discutimos a *aparar* palavra-chave.

RESOLV_ADD_TRIM_DOMAINS

Esta variável especifica uma lista de domínios da guarnição que são adicionados aos valores indicados no *host.conf*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O arquivo nsswitch.conf

A versão 2 da biblioteca GNU padrão inclui uma substituição mais poderosa e flexível para os mais velhos *host.conf* mecanismo. O conceito de serviço de nome foi estendido para incluir uma variedade de diferentes tipos de informação. As opções de configuração para todas as diferentes funções que consultar esses bancos de dados foram trazidos para trás em um único arquivo de configuração, o *nsswitch.conf* arquivo.

A *nsswitch.conf* arquivo permite que o administrador do sistema para configurar uma grande variedade de bases de dados diferentes. Nós limitar nossa discussão a opções relacionadas ao acolhimento e resolução de endereços de rede IP. Você pode facilmente encontrar mais informações sobre os outros recursos através da leitura da documentação do GNU biblioteca padrão.

Opções na *nsswitch.conf* deve aparecer em linhas separadas. Os campos podem ser separados por espaços (espaços ou tabulações).
A cerquilha (#) Apresenta um comentário que se estende até o fim da linha. Cada linha descreve um determinado serviço; resolução de nomes é um desses. O primeiro campo em cada linha é o nome do banco de dados, terminando com dois pontos. O nome do banco de dados associados com a resolução de endereço de host é *hosts*. Um banco de dados relacionados é *redes*, Que é utilizado para a resolução de nomes de rede em endereços de rede. O restante das lojas de cada linha de opções que determinam as pesquisas caminho para o banco de dados são executadas.

As opções disponíveis são as seguintes:

dns

> Use o Domain Name System (DNS) para resolver o endereço. Isso faz sentido apenas para anúncios em host Resolução do vestido, não a resolução de endereços de rede. Este mecanismo utiliza a */ Etc / resolv.conf* arquivo que vamos descrevemos mais adiante neste capítulo.

arquivos

> Procurar um arquivo local para o nome do host ou rede e seu endereço correspondente. Esta opção usa o tradicionais tra- */ Etc / hosts* e */ Etc / network* arquivos.

nis ou *nisplus*

> Utilize o Network Information System (NIS) para resolver o host ou o endereço de rede. NIS e NIS + é discutidos em detalhe no Capítulo 13, *O Sistema de Informação de Rede*.

A ordem em que os serviços a serem consultados estão listados determina a ordem em que eles são consultados quando tentar resolver um nome. A lista de pedidos de consulta é na descrição de serviço na */ Etc / nsswitch.conf* arquivo. A serviços são consultados a partir da esquerda para a direita e, por padrão procura pára quando uma resolução é bem-sucedido.

Um exemplo simples de acolhimento e especificação de banco de dados de rede que imitaria a nossa configuração usando o velhas biblioteca padrão libc é mostrado na Exemplo 6.2.

Exemplo 6.2: Exemplo de arquivo nsswitch.conf

```
# / Etc / nsswitch.conf
#
# Exemplo de configuração do nome GNU funcionalidade Service Switch.
# Informações sobre este arquivo está disponível em `libc6-doc '.

hosts:          arquivos dns
redes:          arquivos
```

Este exemplo faz com que o sistema de olhar para cima acolhe a primeira no Domain Name System, e as */ Etc / hosts* arquivo, que se não pode encontrá-los. pesquisas de nome de rede seria tentada usando apenas o */ Etc / networks* arquivo.

Você é capaz de controlar o comportamento de pesquisa, mais precisamente com "itens de ação", que descreve as medidas a tomar tendo em conta o resultado da tentativa anterior de pesquisa. Os itens de ação aparecem entre as especificações de serviços, e são

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

incluído dentro de colchetes, *[]*. A sintaxe geral da instrução de ação é:

`[[!]` *status* `=` *ação* `...]`

Há duas ações possíveis:

retorno

Controls retorna para o programa que tentou a resolução de nomes. Se uma pesquisa tentativa foi bem sucedida, o resolvedor vai retornar com os detalhes, caso contrário ele irá retornar um resultado zero.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

continua

r A resolução vai passar para o próximo serviço de resolução lista e tentar usá-lo.

(!) O caráter opcional especifica que o valor de status deve ser invertida antes do teste, isto é, significa "não".

Os valores disponíveis no estado que podemos atuar são:

sucesso

A entrada solicitado foi encontrado sem erros. A ação padrão para este estado é *retorno*.

notfound

Não houve erro na pesquisa, mas o host de destino ou a rede não pôde ser encontrado. A ação padrão para este estado é *continuar*.

unavail

O serviço foi consultado indisponíveis. Isto poderia significar que o *hosts* ou *redes* arquivo foi ilegível para o *arquivos* serviço ou que um servidor de nomes ou servidor NIS não respondeu para o *dns* ou *nis* serviços. O de-ação de falha para este estado é *continuar*.

tryagain

Esse status significa que o serviço está temporariamente indisponível. Para o *arquivos* serviço de arquivos, isso

normalmente seria
indicar que o arquivo foi bloqueado por causa de algum processo. Para outros serviços, pode significar o servidor foi temporariamente incapaz de aceitar conexões. A ação padrão para este estado é *continuar*.

Um exemplo simples de como você pode usar esse mecanismo é mostrado na Exemplo 6.3.

Exemplo 6.3: Exemplo de arquivo nsswitch.conf Usando uma Declaração de Ação

```
# / Etc / nsswitch.conf
#
# Exemplo de configuração do nome GNU funcionalidade Service Switch.
# Informações sobre este arquivo está disponível em `libc6-doc '.

hosts:          dns [! unavail = return] files
redes:          arquivos
```

Este exemplo tentativas de resolução de host usando o Domain Name System Service. Se o status de retorno é nada além indisponível, o resolvedor retorna o que encontrou. Se, e somente se, a pesquisa de DNS retorna tentativa um status indisponível, o resolvedor tenta usar o local */ Etc / hosts*. Isto significa que devemos usar o *hosts* arquivo somente se o servidor de nomes não está disponível por algum motivo.

Nome pesquisas Configurando Server Usando resolv.conf

Ao configurar a biblioteca de resolução para usar o serviço do BIND para pesquisas de host, você também tem que falar isso que os servidores de nome para usar. Há um arquivo separado para esta chamada *resolv.conf*. Se este arquivo não existe ou é vazio, o resolvedor assume o nome do servidor está em sua máquina local.

Para executar um servidor de nome do seu host local, você terá de configurá-lo separadamente, como será explicado a seguir seção. Se você estiver em uma rede local e ter a oportunidade de usar um servidor de nome existente, este deve sempre ser o preferido. Se você usar uma conexão dial-up IP para a Internet, que, normalmente, especificar o nome do servidor seu provedor de serviços na *resolv.conf* arquivo.

A opção mais importante na *resolv.conf* é *servidor de nomes*, Que fornece o endereço IP de um servidor de nome para usar. Se você especificar vários servidores de nome, dando a *servidor de nomes* várias vezes opção, eles são julgados pela ordem dado. Você deve colocar o servidor mais confiável em primeiro lugar. A implementação atual permite que você tenha até a três *servidor de nomes* declarações *resolv.conf*. Se não *servidor de nomes* opção é dado, o resolvedor tenta se conectar para o nome do servidor no host local.

Duas outras opções, *domínio* e *pesquisa*, Vamos usar nomes de atalho para os hosts em seu domínio local. Normalmente, quando apenas um telnet para outro host no seu domínio local, você não quer digitar o nome totalmente qualificado, mas use um nome como *gauss* na linha de comando e ter a aderência de resolução sobre a *mathematics.groucho.edu* peça.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Este é apenas o *domínio* finalidade instrução. Ele permite que você especifique um nome de domínio padrão a ser anexado ao DNS
falha ao procurar um nome. Por exemplo, quando recebe o nome *gauss*, O resolvedor não localizar *gauss.* no DNS,
porque não há nenhum domínio de nível superior como. Quando administrado *mathematics.groucho.edu* como um domínio padrão, o re-
solver repete a consulta para *gauss* com o domínio padrão anexa, desta vez bem sucedido.

Isso é ótimo, você pode pensar, mas assim que você sair do domínio do departamento de matemática, você está de volta aos nomes totalmente qualificados. É claro, você também quer ter como shorthands *quark.physics* para hosts em
domínio do Departamento de Física da.

Isto é, quando o *lista de pesquisa* aparece, uma lista de pesquisa podem ser especificados usando a *pesquisa* opção, que é uma

generali-
zação da *domínio* declaração. Quando este dá um domínio padrão único, o ex especifica uma lista completa
deles, cada um a ser julgado por sua vez, até que uma pesquisa bem-sucedida. Essa lista deve ser separado por espaços em branco ou tabs.

A *pesquisa* e *domínio* declarações são mutuamente exclusivos e não podem aparecer mais de uma vez. Se nenhuma opção é dado, a resolução irá tentar adivinhar o domínio padrão a partir do host local utilizando a *getdomainname (2)*
sistema de chamada. Se o host local não tem uma parte do domínio, o domínio padrão será assumido como sendo a raiz domínio.

Se você decidir colocar uma *pesquisa* declaração em *resolv.conf*, Você deve ser cuidadoso sobre o que você adicionar a

domínios
esta lista. Resolver bibliotecas antes BIND 4,9 usados para construir uma lista de busca padrão do nome de domínio quando nenhuma lista de busca foi dada. Esta lista foi composta por padrão do domínio padrão em si, além de todos os domínios de seu pai
até a raiz. Isso causou alguns problemas porque as solicitações de DNS dissolvida em servidores de nomes que nunca foram quis vê-los.

Suponha que você está na Cervejaria Virtual e quero fazer login para *foot.groucho.edu*. Por um deslize de seus dedos, você erra *pé* como *foo*, Que não existe. GMU servidor de nome, portanto, dizer-lhe que não conhece esses hosts.
Com a lista de pesquisa de estilo antigo, o resolvedor iria agora a tentar com o nome *vbrew.com* e *com* anexado.
O último é problemático, porque *groucho.edu.com* pode realmente ser um nome de domínio válido. Do servidor de nomes poderia, então, até encontrar *foo* em seu domínio, apontando-lhe um dos seus anfitriões - o que claramente não foi planejado.

Para algumas aplicações, essas pesquisas falsas host pode ser um problema de segurança. Portanto, você deve geralmente

limitam
os domínios em sua lista de busca à sua organização local, ou algo semelhante. Na matemática de-
partamento de Groucho Marx universidade, a lista de pesquisa seria normalmente ser definido como *maths.groucho.edu* e *groucho.edu*.

Se domínios padrão de som confuso para você, considere este exemplo *resolv.conf* arquivo para a Cervejaria Virtual:

```
# / Etc / resolv.conf
# O nosso domínio
domínio        vbrew.com
#
# Nós usamos o vlager como servidor de nomes central:
servidor de     172.16.1.1
nomes
```

Ao resolver o nome *Vale*, O resolvedor olha para cima *Vale* e, na falta deste, *vale.vbrew.com*.

Resolver Robustez

Ao executar uma LAN dentro de uma rede maior, você definitivamente deve usar nomes de servidores centrais, se eles estão dis-
capaz. Os servidores de nomes desenvolver caches rica que as consultas repetir acelerar, uma vez que todas as consultas são encaminhadas para eles.
No entanto, este regime tem um inconveniente: quando um incêndio destruiu o cabo de backbone na universidade Olaf, nada mais
trabalho foi possível em LAN do seu departamento, porque a resolução já não podia chegar a qualquer dos servidores de nome.
Esta situação provocou dificuldades com a maioria dos serviços de rede, como logins terminal X e impressão.

Embora não seja muito comum para backbones campus para ir para baixo em chamas, você deve sempre tomar precauções

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

contra casos como este.

Uma opção é montar um servidor de nomes que resolve nomes de host do seu domínio local e encaminha todas as consultas para outros nomes de máquinas para os servidores principais. Claro, isso só é aplicável se você estiver executando o seu próprio
domínio.

Alternativamente, você pode manter uma tabela de host de backup para o seu domínio ou em LAN */ Etc / hosts*. Isto é muito simples de fazer. Você simplesmente garantir que a biblioteca de resolução de consultas ao DNS por um lado, e os anfitriões do próximo arquivo. Em um */ Etc / host.conf* arquivo

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

você pode usar "*order bind, hosts*"E, em um */ Etc / nsswitch.conf* arquivo que você usaria "*hosts: files dns*",

Para fazer o resolvedor
cair de volta para o arquivo hosts, se o nome do servidor central é inacessível.

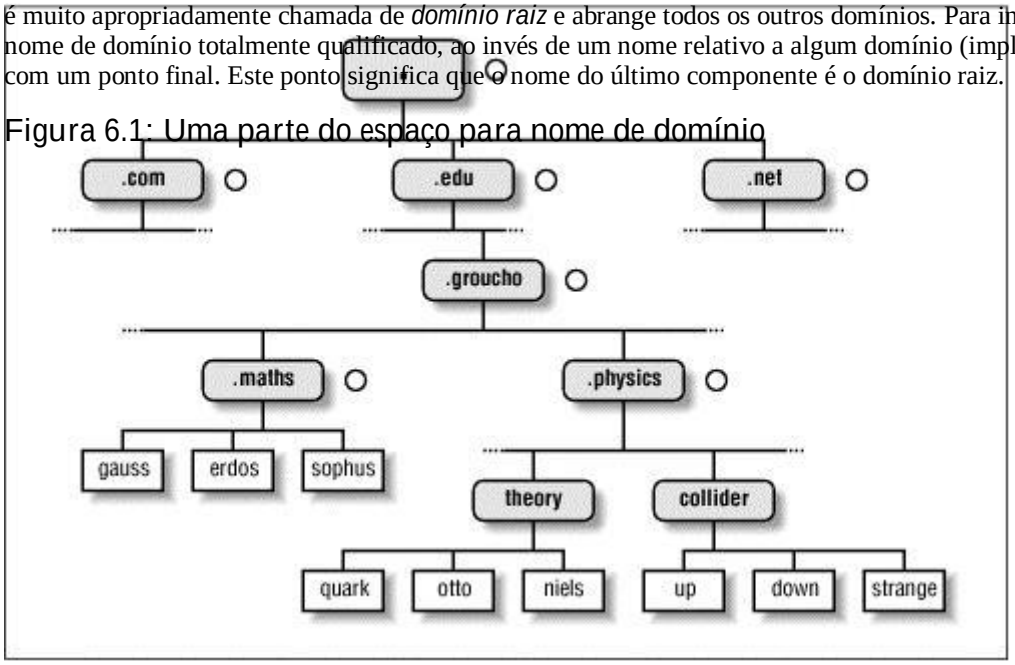
Como funciona o DNS

DNS organiza hostnames em uma hierarquia de domínio. A *domínio* é uma coleção de sites que estão

relacionados de alguma
sentido - porque eles formam uma rede adequada (por exemplo, todas as máquinas em um campus, ou todos os hosts na BITNET), porque
todas elas pertencem a uma determinada organização (por exemplo, o governo dos EUA), ou porque são simplesmente geograficamente
fechar. Por exemplo, as universidades são comumente agrupadas na *edu* domínio, com cada universidade ou faculdade usando separado *subdomínio*, Abaixo do qual os seus anfitriões são subsumidas. Groucho Marx Universidade tem a *groucho.edu* domínio, enquanto a LAN do departamento de Matemática é atribuída *maths.groucho.edu*. Hosts no departmen-
Tal rede teria esse nome de domínio tacked para seu host, então *Erdos* seria conhecido como *erdos.maths.groucho.edu*. Este é o chamado *totalmente qualificado nome de domínio* (FQDN), que identifica esse
acolhimento a nível mundial.

Figura 6.1 scomos uma secção do espaço. A entrada na raiz desta árvore, que é indicado por um único ponto,
é muito apropriadamente chamada de *domínio raiz* e abrange todos os outros domínios. Para indicar que uma máquina é uma nome de domínio totalmente qualificado, ao invés de um nome relativo a algum domínio (implícito) local, às vezes, é escrito com um ponto final. Este ponto significa que o nome do último componente é o domínio raiz.

Figura 6.1: Uma parte do espaço para nome de domínio



Dependendo de sua localização na hierarquia de nome, um domínio pode ser chamado de nível superior, de nível secundário, ou de terceiro nível.
Mais níveis de subdivisão ocorrer, mas elas são raras. Esta lista detalha vários domínios de nível superior você pode ver fre-temente:

Domínio edu	Descrição net
com	

org

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

(Principalmente dos EUA) instituições de ensino como universidades.	e empresas. As organizações não-comercial. As redes privadas UUCP são frequentemente neste domínio.
As organizações comerciais	Gateways e outros hosts administrativos de uma rede.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Domínio	Descrição
mil	instituições militares dos EUA.
gov	instituições governamentais dos EUA.
uucp	Oficialmente, todos os nomes dos sites anteriormente utilizadas como nomes de domínios UUCP sem ter sido movido para este domínio.

Historicamente, as primeiras quatro destas foram distribuídos para os EUA, mas as mudanças recentes na política fizeram com que estes
domínios, denominada global Domínios de Alto Nível (gTLDs), são agora considerados de natureza global. As negociações estão cur-
atualmente em andamento para ampliar o leque de gTLDs, que pode resultar em uma maior escolha no futuro.

Fora os EUA, cada país usa, geralmente, um domínio de nível superior de seu próprio nome do país de duas letras código definido na norma ISO-3166. Finlândia, por exemplo, usa o *fi* domínio; *fr* é usado pela França, *de* pela Alemanha, e *au* pela Austrália. Abaixo deste domínio de nível superior, o NIC de cada país é livre de organizar hostnames de qualquer maneira eles querem. A Austrália tem domínios de segundo nível semelhante aos domínios internacionais de nível superior, nomeados *com.au* e
edu.au. Outros países, como Alemanha, não utilize este nível extra, mas têm nomes pouco tempo que se referem diretamente a organizações que executam um determinado domínio. Não é incomum ver hostnames como *ftp.informatik.uni-erlangen.de*. Giz que até a eficiência alemã.

É claro que esses domínios nacionais não implicam que uma série desse domínio é realmente localizado no referido país; significa apenas que o anfitrião foi registrado com NIC daquele país. A fabricante sueca pode ter uma filial na Austrália e ainda ter todos os seus hosts registrados com o *se* domínio de nível superior.

Organizar o espaço em uma hierarquia de nomes de domínio bem resolve o problema da exclusividade de nome, com DNS, esse nome tem de ser único apenas dentro de seu domínio para lhe dar um nome diferente de todos os outros hosts no mundo
de largura. Além disso, nomes totalmente qualificados são fáceis de lembrar. Tomado por si só, já são muito boas razões para dividir um grande domínio em vários subdomínios.

DNS faz ainda mais para você do que isso. Ele também permite delegar autoridade sobre um subdomínio à sua adminis-tradores. Por exemplo, os mantenedores, no Centro de Computação Groucho poderia criar um subdomínio para cada de-compartimento, que já encontrou o *matemática* e *física* subdomínios acima. Quando localizar a rede no Departamento de Física muito grande e caótica de gerir de fora (afinal, os físicos são conhecidos por ser um rebelde grupo de pessoas), eles podem simplesmente passar o controle da *physics.groucho.edu* domínio para os administradores deste rede. Esses administradores são livres para usar o host que eles gostam e atribuí-los a partir de endereços IP sua rede em qualquer forma que desejarem, sem interferências externas.

Para este fim, o espaço é dividido em *zonas*, Cada um com raiz em um domínio. Note a sutil diferença entre um *zona* e um *domínio*: O domínio do *groucho.edu* abrange todos os hosts na Universidade de Groucho Marx, enquanto a zona *groucho.edu* inclui somente as máquinas que são gerenciadas pelo Centro de Computação diretamente; aqueles no Matemática, a ics departamento, por exemplo. Os anfitriões do Departamento de Física pertencem a uma zona diferente, ou seja, *fís-ics.groucho.edu*. Em Figura 6.1,o início de uma região é marcada por um pequeno círculo à direita do nome de domínio.

Nome pesquisas com o DNS

À primeira vista, todo o domínio e este alarido zona parece fazer resolução de nomes de um negócio muito complicado. Afinal, se nenhuma autoridade central controla o que os nomes são atribuídos a que acolhe, como é uma aplicação humilde deveria saber?

Agora vem a parte realmente genial sobre o DNS. Se você quiser encontrar o endereço IP do *Erdos*, DNS diz: "Vá perguntar as pessoas que gerenciam, e eles vão te dizer. "

Na verdade, o DNS é um banco de dados gigantesco distribuídos. Ele é implementado por servidores de nome chamado fornecer

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

informações que
em um determinado domínio ou conjunto de domínios. Para cada zona, existem pelo menos dois ou, no máximo alguns, o nome de servidores que
manter toda a informação oficial sobre os hosts nessa zona. Para obter o endereço IP do *Erdos*, Tudo que você tem a fazer é contatar o servidor de nome para o *groucho.edu* zona, que irá retornar os dados desejados.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Mais fácil de dizer do que fazer, você poderia pensar. Então, como eu sei como chegar até o servidor de nomes na Groucho Marx Uni-
biodiversidade? Caso seu computador não estiver equipado com um endereço de resolução de oráculo, o DNS oferece para isso, também. Quando
sua aplicação quer para procurar informações sobre *Erdos*, Ele contata um servidor de nomes local, que realiza uma so-
chamada consulta iterativa para ele. Ele começa por enviar uma consulta para um servidor de nomes para o domínio raiz, pedindo o
endereço do *erdos.maths.groucho.edu*. O servidor de nome raiz reconhece que este nome não pertence à sua zona
de autoridade, mas sim para um abaixo do *edu* domínio. Assim, diz-lhe para contactar um *edu* servidor de nome de zona de
mais informações e inclui uma lista de todos *edu* servidores de nomes, juntamente com seus endereços. O servidor de nome local
Em seguida, vá em frente e uma consulta dessas, por exemplo, *a.isi.edu*. De maneira similar ao servidor de nomes de raiz,
a.isi.edu sabe que o *groucho.edu* as pessoas correm de uma zona própria, e aponta para seus servidores. Os locais
nome do servidor, então, apresentar a sua consulta para *Erdos* para um desses, que vai finalmente reconhecer o nome como ser-
anseio de sua zona, e retornar o endereço IP correspondente.

Isto parece um monte de tráfego a ser gerado para procurar um endereço IP desprezível, mas isso é apenas a minúscula
comparação com a quantidade de dados que teria que ser transferido se ainda estivéssemos presos com *HOSTS.TXT*.
Ainda há espaço para melhorar com esse esquema, no entanto.

Para melhorar o tempo de resposta durante as consultas futuras, o nome do servidor armazena as informações obtidas em seu local
cache. Assim, a próxima vez que alguém em sua rede local quer para procurar o endereço de um host na *groucho.edu*
domínio, o servidor de nome irá diretamente para o *groucho.edu* nome do servidor.[40]

Naturalmente, o nome do servidor não vai manter esta informação para sempre, ele irá descartá-lo depois de algum tempo. O expira-
ção do intervalo é chamado de *tempo para viver*, Ou TTL. Cada dado no banco de dados DNS é atribuído como um TTL pelo ad-
ministrators da zona responsável.

Tipos de servidores de nomes

Os servidores de nomes que armazenam todas as informações sobre os hosts dentro de uma zona são chamados *oficial* para esta zona, e alguns,
vezes são referidos como *nome do servidor mestre*. Qualquer consulta de um host dentro desta zona vai acabar em um destes
nome do servidor mestre.

servidores Mestre deve estar muito bem sincronizados. Assim, a zona do administrador de rede deve fazer um dos
primária servidor, que carrega as informações de zona de arquivos de dados e fazer os outros *secundária* servidores, que
transferir os dados de zona do servidor primário em intervalos regulares.

Tendo em servidores de nome várias distribui a carga de trabalho, mas também fornece backup. Quando uma máquina servidora de nome não
de uma forma benigna, como bater ou perder sua conexão de rede, todas as consultas vão cair de volta para os outros servidores. De
Naturalmente, este regime não protegê-lo de mau funcionamento do servidor que produzem respostas erradas a todas as solicitações de DNS,
como de bugs de software no programa próprio servidor.

Você também pode executar um servidor de nome que não está autorizado para qualquer domínio.[41] Isso é útil, como o nome do servidor será
ainda ser capaz de realizar consultas de DNS para os aplicativos que rodam na rede local e cache as informações.
Por isso, é chamado de *somente de cache* servidor.

O banco de dados DNS

Vimos que o DNS não lida apenas com endereços IP de hosts, mas também troca informações sobre serv-nome
ers. bases de dados DNS pode ter, de fato, muitos tipos diferentes de entradas.
A única informação do banco de dados DNS é chamado de *registro de recurso* (RR). Cada registro tem um tipo de

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

associado a ele descrever o tipo de dados que ele representa, e uma classe especifica o tipo de rede que se aplica. Esta última atende às necessidades de diferentes esquemas de endereçamento, como endereços IP (em classe), Hesíodo endereços (usado pelo sistema do MIT Kerberos), e um pouco mais. O tipo de registro é o protótipo de recursos A registro, que associa um nome de domínio totalmente qualificado, com um endereço IP.

O hospedeiro pode ser conhecido por mais de um nome. Por exemplo, você pode ter um servidor que fornece FTP e World Wide Web servidores, o que você dá dois nomes: *ftp.machine.org* e *www.machine.org*. No entanto, um dos Esses nomes devem ser identificado como o funcionário ou *canônico* hostname, enquanto os outros são simplesmente apelidos referem-

40 Se as informações não estavam em cache, então DNS seria tão ineficiente como qualquer outro método, pois cada consulta envolveria o nome de raiz servidores.

41 Bem, quase. Um servidor de nome tem que fornecer, pelo menos, serviço de nomes para *localhost* e pesquisas inversas de *127.0.0.1*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

anel para o nome da máquina oficial. A diferença é que o nome da máquina canônico é o único com uma associada uma re-
cabo, enquanto os outros só tem um registro de tipo CNAME que aponta para o nome de máquina canônico.

Não vamos passar por todos os tipos de discos, mas damos-lhe um breve exemplo. Exemplo 6.4 scomos uma parte do
o domínio de dados que é carregado em o nome dos servidores para o *physics.groucho.edu* zona.

Exemplo 6.4: Um trecho da named.hosts arquivo para o Departamento de Física

```
; Autorizadas Informações sobre physics.groucho.edu.
@  EM  SOA niels.physics.groucho.edu. janet.niels.physics.groucho.edu. {
                  1999090200       ; Número de série
                  360000           ; Atualização
                  3600             ; Repetição
                  3600000          ; Expirar
                  3600             ; Padrão TTL
                }
;
Os servidores
de nome;
              EM    NS       niels
              EM    NS       gauss.maths.groucho.edu.
gauss.maths.groucho.edu. EM 149.76.4.23
;
; Física Teórica (sub-12)
niels         EM    A        149.76.12.1
              EM    A        149.76.1.12
servidor de    EM    CNAME    niels
nomes         EM    A        149.76.12.2
otto          EM    A        149.76.12.4
quark         EM    A        149.76.12.5
baixo         EM    A        149.76.12.6
estranho
...
; Laboratório Collider.
(Sub-14)                     149.76.14.1
boson         EM    A
muon          EM    A        149.76.14.7
bogon         EM    A        149.76.14.12
...
```

Além dos registros A e CNAME, você pode ver um registro especial no início do arquivo, estendendo-se várias linhas. Este é o registro de recurso SOA da sinalização *Start of Authority*, Que contém informações gerais sobre o zona do servidor é autoritativo para. O registro SOA inclui, por exemplo, o tempo padrão de viver para todos os re-
cordas.

Note-se que todos os nomes no arquivo de exemplo que não terminam com um ponto deve ser interpretado com relação ao *fís-
ics.groucho.edu* domínio. O nome especial (@) Utilizados na SOA registro se refere ao nome de domínio por si só.

Já vimos anteriormente que os servidores de nome para o *groucho.edu* domínio de alguma forma tem que saber sobre o *física* zona, para que possam apontar as consultas para seus servidores de nome. Isto normalmente é alcançado por um par de registros: o NS
registro que dá FQDN do servidor, e um registro que associa um endereço com esse nome. Uma vez que estes re-
cabos são o que mantém o espaço para juntos, eles são freqüentemente chamados de *cola registros*. Eles são os únicos exemplos de registros em que uma zona pai realmente tem informações sobre os hosts na zona subordinada. Os registros de cola apontando para os servidores de nome para *physics.groucho.edu* são mostrados na Exemplo 6.5.

Exemplo 6.5: Um trecho da named.hosts arquivo para GMU

```
; Dados de zona para zona groucho.edu.
@  EM  SOA vax12.gcc.groucho.edu. joe.vax12.gcc.groucho.edu. {
                     1999070100       ; Número de série
                     360000           ; Atualização
                     3600             ; Repetição
                     3600000          ; Expirar
                     3600             ; Padrão TTL
                   }
 ....
```


PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
; Cola registros para a zona physics.groucho.edu
física          EM      NS        niels.physics.groucho.edu.
                EM      NS        gauss.maths.groucho.edu.
niels.physics   EM      A         149.76.12.1
gauss.maths     EM      A         149.76.4.23
...
```

Pesquisas Reversas

Encontrar o endereço IP que pertence a um host é sem dúvida o uso mais comum para o Domain Name System, mas às vezes você vai querer encontrar o nome de máquina canônico correspondente a um endereço. Encontrar esse host é chamada *mapeamento reverso*, E é usado por vários serviços de rede para verificar a identidade de um cliente. Ao utilizar um único *hosts* arquivo, as pesquisas inversas envolver simplesmente pesquisando o arquivo para uma máquina que possui o endereço IP em causa. Com DNS, uma busca exaustiva do espaço de nomes está fora de questão. Em vez disso, um domínio especial, *in-addr.arpa*, Tem foi criado que contém os endereços IP de todos os hosts em uma notação decimal pontilhada revertida. Por exemplo, um IP endereço do *149.76.12.4* corresponde ao nome *-addr.arpa 4.12.76.149.in*. O tipo de registro de recurso de vinculação esses nomes para os seus hostnames canônico é PTR.

Criação de uma zona de autoridade geralmente significa que os seus administradores têm total controle sobre como eles atribuir ad- vestidos para nomes. Uma vez que eles geralmente têm uma ou mais redes ou sub-redes IP em suas mãos, há um um-para-mapeamento de muitos entre as zonas de DNS e redes IP. O Departamento de Física, por exemplo, compreende a sub-redes *149.76.8.0*,*149.76.12.0*E *149.76.14.0*.

Consequentemente, novas zonas na *in-addr.arpa* domínio tem que ser criado junto com o *física* zona, e dele-gate para os administradores de rede no departamento: *-addr.arpa 8.76.149.in*,*-addr.arpa 12.76.149.in*E *-addr.arpa 14.76.149.in*. Caso contrário, a instalação de um novo hospedeiro no Laboratório Collider seria obrigá-los a manter contato com seus domínio pai para ter o novo endereço entrou em sua *in-addr.arpa* arquivo de zona.

O banco de dados da zona para sub-12 é mostrado na Exemplo 6.6.O correspondente cola registros no banco de dados sua zona-mãe são mostrados na Exemplo 6.7.

Exemplo 6.6: Um trecho da named.rev Arquivo de sub-12

```
; O domínio 12.76.149.in addr.arpa.
@  EM  SOA  niels.physics.groucho.edu. janet.niels.physics.groucho.edu. {
                    1999090200 360000 3600 3600000 3600
          }
2         EM      PTR       otto.physics.groucho.edu.
4         EM      PTR       quark.physics.groucho.edu.
5         EM      PTR       down.physics.groucho.edu.
6         EM      PTR       strange.physics.groucho.edu.
```

Exemplo 6.7: Um trecho da named.rev Arquivo para a Rede 149,76

```
; O domínio 76.149.in addr.arpa.
@  EM  SOA vax12.gcc.groucho.edu. joe.vax12.gcc.groucho.edu. {
                    1999070100 360000 3600 3600000 3600
                }
...
, 4 sub-rede: Departamento de Matemática
1.4         EM      PTR       sophus.maths.groucho.edu.
17.4        EM      PTR       erdos.maths.groucho.edu.
23.4        EM      PTR       gauss.maths.groucho.edu.
...
; Sub-12: Departamento de Física, uma das zonas separadas
12          EM      NS        niels.physics.groucho.edu.
            EM      NS        gauss.maths.groucho.edu.
niels.physics.groucho.edu. EM  Um 149.76.12.1
gauss.maths.groucho.edu. EM     A   149.76.4.23
...
```

in-addr.arpa zonas sistema só pode ser criado como supersets de redes IP. Uma restrição ainda mais severa é a máscaras que estas redes têm que ser nos limites de byte. Todas as sub-redes em Groucho Marx Universidade tem um

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

máscara de rede *255.255.255.0*, Portanto uma *in-addr.arpa* zona podem ser criados para cada sub-rede. No entanto, se a rede estiver

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

máscara foram *255.255.255.128* em vez disso, a criação de zonas para a sub-rede *149.76.12.128* seria impossível, porque não há nenhuma maneira de dizer que o DNS *-addr.arpa 12.76.149.in* domínio foi dividido em duas zonas de autoridade, com nomes que variam de *1* através *127*E *128* através *255*, Respectivamente.

Correndo nomeado

`nomeado` (Pronuncia-se *nome-dee*) Fornece DNS na maioria das máquinas Unix. É um programa servidor originalmente desen- desenvolvidos para o BSD fornecer serviço de nome de clientes e, possivelmente, a outros servidores de nomes. BIND Versão 4 foi
há algum tempo e apareceu na maioria das distribuições Linux. A nova versão, a versão 8, foi introduzida
na maioria das distribuições Linux, e é uma grande mudança em relação às versões anteriores.[42] Ele tem muitas características novas, tais como
suporte para atualizações de DNS dinâmico, as notificações de alteração de DNS, o desempenho melhorou muito, e uma nova configuração será
ração sintaxe do arquivo. Verifique a documentação contida na distribuição do código fonte para maiores detalhes.

Esta seção requer alguma compreensão do modo como DNS funciona. Se a discussão está tudo grego para você,
você pode querer reler a seção "Como o DNS funciona.

`nomeado` geralmente tem início no momento da inicialização do sistema e vai até a máquina vai para baixo novamente.

Implementações de
BIND anteriores à versão 8 tomar as suas informações de um arquivo de configuração chamado `/ Etc / named.boot` e vari-
ous arquivos que mapeiam nomes de domínio para endereços. Estes últimos são chamados *arquivos de zona*. As versões do BIND versão 8
A partir de uso */ Etc / named.conf* em lugar de */ Etc / named.boot*.

Para executar `nomeado` no prompt, digite:

```
# / Usr / sbin / named
```

`nomeado` virão para cima e ler a `named.boot` arquivo e qualquer arquivos de zona especifica. Ele grava o seu processo ID para */ Var / run / named.pid* em ASCII, downloads de todos os arquivos de zona dos servidores primário, se necessário, e inicia-lis
tening na porta 53 para consultas DNS.

O arquivo named.boot

O arquivo de configuração BIND anteriores à versão 8 foi muito simples na estrutura. BIND versão 8 possui um muito dife- sintaxe do arquivo ent configuração para lidar com muitas das novas funcionalidades introduzidas. O nome da configuração arquivo foi alterado de */ Etc / named.boot*, Em versões mais antigas do BIND, para */ Etc / named.conf* na versão do BIND 8. Nós foco sobre a configuração a versão mais antiga, pois é provavelmente o que a maioria das distribuições ainda estão usando, mas vamos
apresentar uma equivalência *named.conf* para ilustrar as diferenças, e vamos falar sobre como converter o formato antigo para o novo.

A `named.boot` arquivo geralmente é pequena e contém pouco, mas os ponteiros para arquivos mestres zona contendo infor- ção e ponteiros para outros servidores de nomes. Comentários no início do arquivo de boot com o (#) ou (;) caracteres, e estender para o fim da linha. Antes de discutir o formato do *named.boot* em detalhes, vamos dar uma olhada no exemplo arquivo para *vlager* dada em Exemplo 6.8.

Exemplo 6.8: A named.boot arquivo para vlager

```
;
; Arquivo / etc named.boot / para vlager.vbrew.com
;
Diretório     / Var / named
;
;             domínio                 arquivo
;-----------------
cache         .                       named.ca
primária            primária          vbrew.com
primária                              0.0.127.in-addr.arpa
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
-addr.arpa 16.172.in named.hosts
                    named.local
                    named.rev
```

[42] BIND 4,9 foi desenvolvido por Paul Vixie, paul@vix.com, mas o BIND é agora mantido pelo Internet Software Consortium, ligam-bugs@isc.org.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Vamos olhar para cada instrução individualmente. A *Diretório* palavra-chave diz nomeado que todos os nomes referidos mais tarde
neste arquivo, os arquivos de zona, por exemplo, estão localizados na */ Var / named* diretório. Isso economiza um pouco de digitação.

A *primária* palavra-chave mostrado neste exemplo carrega informações em nomeado. Essas informações são obtidas a partir da
Os arquivos mestres especificado como o último dos parâmetros. Esses arquivos representam os registros de recursos DNS, que será
olha seguinte.

Neste exemplo, nós configuramos nomeado como o servidor primário de nomes para três domínios, tal como indicado pelos

três
primária declarações. A primeira destas declarações instrui nomeado para atuar como um servidor primário *vbrew.com*, Tak-
ção os dados da zona a partir do arquivo *named.hosts*.

A *cache* palavra-chave é muito especial e deve estar presente em praticamente todas as máquinas rodando um servidor de nome.

É
instrui nomeado para permitir a sua cache e carregar o *dicas de raiz do servidor de nomes* a partir do arquivo de cache especificado (*named.ca* no nosso exemplo). Vamos voltar para as dicas de nome do servidor na lista a seguir.

Aqui está uma lista das opções mais importantes que você pode usar em *named.boot*:

Diretório

Esta opção especifica um diretório no qual residem os arquivos de zona. Os nomes de arquivos em outras opções

podem ser
dado em relação a este diretório. Diversos diretórios podem ser especificados usando repetidamente *Diretório*. A Sistema de arquivos padrão do Linux sugere que este deve ser */ Var / named*.

primária

Esta opção tem um nome de domínio eo nome do arquivo como um argumento, declarando que o local servidor

autoritativo
para o domínio. Como um servidor primário, nomeado carrega as informações de zona do mestre dado
arquivo.

Sempre haverá pelo menos um *primária* entrada em cada inicialização de arquivo usado para mapeamento reverso da

rede
127.0.0.0, Que é a rede de loopback local.

secundária

Esta afirmação tem um nome de domínio, uma lista de endereços, e um nome de arquivo como um argumento. Ele

declara o local
servidor de um servidor mestre secundário para o domínio especificado.

Um servidor secundário possui dados conclusivos sobre o domínio, também, mas não recolhê-lo a partir de arquivos, em vez

disso, ele tenta
para fazer o download do servidor primário. O endereço IP de pelo menos um servidor primário, portanto, deve ser dada à nomeado na lista de endereços. Os contatos do servidor local de cada um deles por sua vez, com sucesso, até que transfira a zona
banco de dados, que é então armazenado no arquivo de backup dado como o terceiro argumento. Se nenhum dos servidores principais re-
ponde, os dados da zona são recuperados do arquivo de backup em vez disso.

nomeado Em seguida, tenta atualizar os dados da zona em intervalos regulares. Esse processo é explicado mais tarde, em

conexão
com o tipo de registro de recurso SOA.

cache

Esta opção tem um nome de domínio eo nome do arquivo como argumentos. Este arquivo contém as sugestões de

servidores-raiz,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

que é uma lista de registros apontando para os servidores de nome raiz. Somente registros NS e A será reconhecido. A *domínio* deve ser o nome do domínio raiz, de um período simples (.).

Esta informação é absolutamente crucial para `nomeado`; Se o *cache* declaração de não ocorrer no arquivo de

inicialização,
`nomeado` não vai desenvolver um cache local em tudo. Esta situação / falta de desenvolvimento irá degradar severamente
desempenho e carga da rede aumentar se o próximo servidor consultado não está na rede local. Além disso,
`nomeado` não será capaz de atingir todos os servidores de nomes de raiz e, portanto, não resolverá todos os endereços excepto
aqueles que tem autoridade para. Uma exceção a esta regra envolve servidores de encaminhamento (ver o *encaminhadores*
opção que se segue).

encaminhadores

Esta afirmação tem uma lista separada por espaços de endereços como um argumento. Os endereços IP neste
lista especificar uma lista de servidores de nomes que `nomeado` podem consultar se ele não consegue resolver uma consulta a partir do seu local
cache. Eles são julgados em ordem, até que um deles responde a uma consulta. Normalmente, você usaria o
nome do servidor de seu provedor de rede ou outro servidor conhecido como um encaminhador.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

escravo

Esta declaração faz com que o servidor de um nome *escravo* servidor. Nunca realiza consultas recursivas em si, mas apenas
encaminha-los para os servidores especificados no *encaminhadores* declaração.

Existem duas opções que não vou descrever aqui: *sortlist* e *domínio*. Duas outras diretrizes também podem ser utilizados dentro desses arquivos de banco de dados: *$ INCLUDE* e *$ ORIGIN*. Uma vez que eles raramente são necessários, não vamos descrevê-los
aqui, também.

O BIND 8 host.conf Arquivo

BIND versão 8 introduziu uma série de novas funcionalidades, e com isso veio uma sintaxe novo arquivo de configuração. A *named.boot*, Com a sua simples declarações única linha, foi substituído pelo *named.conf* arquivo, com uma sintaxe como a de `gated` e lembrando C sintaxe fonte.

A nova sintaxe é mais complexa, mas, felizmente, uma ferramenta tem sido desde que automatiza a conversão do sintaxe antiga para a nova sintaxe. No pacote de fonte de BIND 8, a `perl` programa chamado `named-bootconf.pl` é desde que vai ler o seu vigor *named.boot* arquivo da `stdin` e convertê-lo para o equivalente *named.conf* formato eletrônico em `stdout`. Para usá-lo, você deve ter o `perl` interpretador instalado.

Você deve usar o script mais ou menos assim:

```
# cd / etc
# named.conf> named-bootconf.pl <named.boot
```

O script então produz um *named.conf* que se parece com o mostrado na Exemplo 6.9.Já limpou algumas das comentários úteis inclui o script para ajudar a mostrar a relação quase direta entre o velho eo novo sintaxe.

Exemplo 6.9: O BIND named.conf equivalente de 8 de arquivo para vlager

```
/ /
/ / / Arquivo named.boot etc / para vlager.vbrew.com
options {
        diretório "/ var / named";
};

zone "." {
        dica do tipo;
        arquivo "named.ca";
};

"Vbrew.com" zona {
        type master;
        arquivo "named.hosts";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        arquivo "named.local";
};

zone "16.172.in-addr.arpa" {
        type master;
        arquivo "named.rev";
};
```

Se você der uma olhada de perto, verá que cada uma das afirmações de uma linha em *named.boot* foi convertido em uma declaração C-como fechado dentro de {} caracteres no *named.conf* arquivo.

Os comentários, que no *named.boot* ficheiro de ter sido indicado por um ponto e vírgula (;), são agora indicados por dois para-barras ala (//).

A *Diretório* declaração foi traduzida para um *opções* parágrafo com um *Diretório* cláusula.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A *cache* e *primária* declarações foram convertidos em *zona* parágrafos com *tipo* cláusulas do *sugestão* e *MAS-ter*, Respectivamente.

Os arquivos de zona não precisa ser modificado de forma alguma, sua sintaxe permanece inalterada.

A sintaxe da nova configuração permite muitas novas opções que não temos abordado aqui. Se você gostaria de informações sobre as novas opções, a melhor fonte de informação é a documentação fornecida com a versão do BIND 8 origem do pacote.

O DNS arquivos de banco

arquivos Master incluído `nomeado`, Como `named.hosts`, Sempre têm um domínio a eles associados, que é chamada *origem*. Este é o nome de domínio especificado com o *cache* e *primária* opções. Dentro de um arquivo mestre, você pode especificar nomes de domínio e de acolhimento em relação a este domínio. Um nome dado em um arquivo de configuração
é considerado *absoluta* Se terminar em um único ponto, caso contrário ele é considerado em relação à origem. A origem de em si pode ser encaminhado à utilização (@).

Os dados contidos em um arquivo mestre é dividido em *registros de recursos*(RR). RRs são as menores unidades de informação disponíveis através do DNS. Cada registro tem um tipo de recurso. Registros, por exemplo, mapear um hostname para um endereço IP
endereço, e um registro CNAME associa um apelido para um host com o nome do host oficial. Para ver um exemplo, veja em Exemplo 6.11, que mostra a `named.hosts` arquivo mestre para a cervejaria virtual.

representações registro de recurso em arquivos mestres compartilham um formato comum:

[*domínio*[ ]*ttl*[ ]*classe*] *rdata tipo*

Os campos são separados por espaços ou tabulações. Uma entrada pode ser continuado em várias linhas, se uma chave de abertura ocorre
antes da nova linha primeiro e do último campo é seguido por uma chave de fechamento. Qualquer coisa entre um ponto e vírgula e um
nova linha é ignorada. A descrição das condições formato seguinte:

domínio

Este termo é o nome de domínio para o qual a entrada se aplica. Se nenhum nome de domínio é dado, o RR é tão-sumidos a aplicar-se o domínio do RR anterior.

ttl

A fim de forçar resolvedores para descartar as informações após um determinado tempo, cada RR está associado um tempo para
ao vivo (*ttl*). O campo TTL especifica o tempo em segundos que a informação é válida depois de ter sido re-Extraído de servidor. É um número decimal com no máximo oito dígitos.

Se nenhum valor ttl for dada, o valor padrão para esse campo do *mínimo* domínio da re-SOA anterior cabo.

classe

Esta é uma classe de endereços, como dentro para endereços IP ou SH para objetos na classe de Hesíodo. Para TCP líquida / IP-
de trabalho, você tem que especificar IN.

Se nenhum campo de classe é dado, a classe do RR precedente é assumida.

tipo

Este artigo descreve o tipo do RR. Os tipos mais comuns são A, SOA, PTR e NS. Os seguintes seções descrevem os diversos tipos de RRs.

rdata

Esta contém os dados associados à RR. O formato deste campo depende do tipo de RR. Na na sequência da discussão, será descrito para cada RR separadamente.

A seguir está a lista parcial de RRS para ser usada em arquivos de DNS mestre. Há mais um par delas que vamos Não explicam, são experimentais e de pouco uso, em geral.

SOA

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Este RR descreve uma zona de autoridade (SOA significa "Start of Authority"). É sinal de que os registros se-
mugido RR SOA conter informação autorizada para o domínio. Cada arquivo mestre incluído por um

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

primária declaração deve conter um registro SOA para esta zona. Os dados de recurso contém o seguinte campos:

origem

Este campo é o hostname canônica do servidor de nome primário para este domínio. Geralmente é dado como um nome absoluto.

contato

Este campo é o endereço de e-mail da pessoa responsável pela manutenção do domínio, com o "@"Sinal substituído por um ponto. Por exemplo, se a pessoa responsável na Cervejaria Virtual foram *janet*, Este campo conteria *janet.vbrew.com*.

série

Este campo é o número da versão do arquivo de zona, expresso em um único número decimal. Sempre que os dados é alterado no arquivo da zona, este número deve ser incrementado. Uma convenção comum é usar um número que reflete a data da última atualização, com um número de versão anexado a ele para cobrir o caso de várias atualizações que ocorrem em um único dia, por exemplo, 2000012600 atualização sendo que 00 ocorreram em janeiro
26, de 2000.

O número de série é usado por servidores de nomes secundário para reconhecer as alterações informações de zona. Para manter-se atualizado,
servidores secundários pedido de registro do servidor primário SOA em determinados intervalos e comparar o número de série o do registro SOA em cache. Se o número mudou, os servidores secundários transferir os dados da zona inteira-base do servidor primário.

refrescar

Este campo especifica o intervalo em segundos que o servidor secundário deve aguardar entre verificando a SOA registro do servidor primário. Novamente, este é um número decimal com no máximo oito dígitos.

Geralmente, a topologia da rede não muda com muita freqüência, de modo que este número deve indicar um intervalo de
cerca de um dia para redes maiores, e mais ainda para os menores.

tentar novamente

Este número determina a periodicidade com que um servidor secundário deve tentar novamente entrar em contato com o primário
servidor, se um pedido ou uma zona de falha de atualização. Não deve ser muito baixo, ou uma falha temporária do servidor ou uma
problema de rede pode causar o servidor secundário para desperdiçar recursos da rede. Uma hora, ou talvez uma hora e meia, pode ser uma boa escolha.

expirar

Este campo especifica o tempo em segundos após o qual um servidor secundário deve, finalmente descartar toda a zona dados se ele não foi capaz de contatar o servidor primário. Você normalmente deve definir este campo para pelo menos um
semana (604.800 segundo), mas aumentando-o para um mês ou mais também é razoável.

mínimo

Este campo é o padrão *ttl* valor para os registros de recursos que não contém explicitamente um. O valor ttl especifica a quantidade máxima de tempo que outros servidores de nomes podem manter o RR no seu cache. Dessa vez só se aplica aos buscas normais, e não tem nada a ver com o tempo após o qual um servidor secundário deve tentar atualizar as informações de zona.

Se a topologia da rede não muda com freqüência, uma semana ou até mais é provavelmente uma boa escolha. Se RRS única mudança com mais freqüência, você ainda pode atribuir-lhes TTLS menores individualmente. Se sua rede muda com freqüência, você pode querer definir *mínimo* para um dia (86.400 segundos).

A

Isto associa gravar um endereço IP com um hostname. O recurso de campo de dados contém o endereço na pontilhada notação decimal.

Para cada host, deve haver apenas um registro. O nome da máquina utilizada neste registro é considerada o funcionário ou *canônico* hostname. Todos os outros nomes de máquinas são apelidos e devem ser mapeados para os

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

ca-
hostname nonical usando um registro CNAME. Se o nome canônico do nosso anfitrião foram vlager, Teríamos um
Um registro que associado que hostname com o seu endereço IP. Uma vez que também pode querer outra associação de nome
ciados com esse endereço, por exemplo *notícias*, A gente criar um registro CNAME que associa o nome com esta alternativa
o nome canônico. Falaremos mais sobre os registros CNAME em breve.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

NS

Os registros NS são usados para especificar servidor primário de uma zona e todos os seus servidores secundários. Um registro NS
aponta para um servidor de nomes mestre da zona determinada, com o campo de dados de recursos contendo o nome do host
do servidor de nomes.

Você vai encontrar registros NS em duas situações: A primeira situação é quando você delegar autoridade a um sub-zona de coordenar, a segunda é no banco de dados da zona master da zona subordinar-se. Os conjuntos de servidores especificados em ambos os pais e as zonas delegadas devem corresponder.

O registro NS especifica o nome dos servidores de nomes primário e secundário para uma zona. Estes nomes
deve ser resolvido para um endereço para que possam ser utilizados. Às vezes, os servidores pertencem ao domínio que estão servindo, o que provoca um "ovo e da galinha" problema, não podemos resolver o endereço até que o nome servidor está acessível, mas não podemos chegar ao servidor de nomes até que nós resolvamos o seu endereço. Para resolver esse di-
Lema, que pode configurar especiais registros diretamente no servidor de nomes da zona pai. O A re-cabos permitem os servidores de nome do domínio pai para resolver o endereço IP do nome da zona delegada servidores. Esses registros são comumente chamados *cola registros* porque fornecem a "cola" que liga um zona delegada a seu pai.

CNAME

Isto associa gravar um alias com uma série de *hostname canônica*. Ele fornece um nome alternativo pelo qual os usuários podem consultar o host cujo nome canônico é fornecido como um parâmetro. O nome do host canônico é o arquivo mestre fornece um registro para; aliases são simplesmente ligados a esse nome por um CNAME registro, mas não tem quaisquer outros registros de suas próprias.

PTR

Este tipo de registro é usado para associar nomes na *in-addr.arpa* com nomes de domínio. É usado para mapeamento reverso de endereços IP para hostnames. O nome da máquina deve ser dado o nome de máquina canônico.

MX

Este RR anuncia um *trocador mail* para um domínio. trocadores Mail são discutidas no "Correio de Encaminhamento . Internet "A sintaxe de um registro MX é:

`[`*domínio*`[]`*ttl*`[]`*classe*`] MX` *preferência hospedeira*

host permutador de nomes para o e-mail *domínio*. Cada troca de mensagens tem um número inteiro *preferência* associado a ele.

A
agente de transporte de correio que pretende entregar correio para *domínio* tenta todos os hosts que têm um registro MX para este domínio
até obter êxito. Aquele com o menor valor de preferência é julgado primeiro, depois as demais, em ordem crescente de preferência de valor.

HINFO

Este registro fornece informações sobre o hardware do sistema e software. Sua sintaxe é:

`[`*domínio*`[]`*ttl*`[]`*classe*`] HINFO` *software e hardware*

A *hardware* campo identifica o hardware utilizado por esta máquina. convenções especiais são usados para especificar isso. Uma

lista
de validade "nomes de máquinas" é dada na RFC Assigned Numbers (RFC-1700). Se o campo contiver espaços em branco, ele deve ser colocado entre aspas duplas. A *software* nomes de campo do software de sistema operacional utilizado pelo sistema. Mais uma vez, um nome válido a partir do RFC Assigned Numbers deve ser escolhido.

Um `HINFO` registro para descrever um processador Intel máquina Linux deve ser algo como:

```
tao   36500  EM  HINFO  IBM-PC  LINUX2.2
```

e `HINFO` registros para Linux rodando em máquinas Motorola 68000-baseado pode parecer:

```
Cevad 36500 IN  HINFO  Atari 104ST LINUX2.0
Jedd  36500 IN  HINFO  AMIGA-3000  LINUX2.0
```

Caching-somente o nome de configuração

Existe um tipo especial de *nomeado* configuração que vamos falar, antes de explicar como criar um nome completo servidor de configuração. Ele é chamado de *somente de cache* configuração. Realmente não servir a um domínio, mas atua como um relé para todas as consultas DNS produzidos no seu host. A vantagem deste esquema é que ele cria uma cache para que apenas os

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

primeira consulta para um determinado host é enviada para os servidores de nomes na Internet. Qualquer pedido será repetido respondidas diretamente do cache no seu servidor de nomes local. Isso pode não parecer útil ainda, mas quando você vai

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

discando para a Internet, conforme descrito no Capítulo 7, *Serial Line IP* eo capítulo 8, *O Proto Point-to-Point-col*.

A*named.boot* arquivo para um servidor somente de cache parecido com este:

```
; Arquivo named.boot para o servidor somente de cache
Diretório                          / Var / named
primária      0.0.127.in-addr.arpa   named.local; rede localhost
cache         .                      named.ca    servidores-raiz;
```

Além desta *named.boot* arquivo, você deve configurar o *named.ca* arquivo com uma lista válida de servidores de nomes raiz.

Você
pode copiar e usar Exemplo 6,10 fou o efeito. Não outros arquivos são necessários para uma configuração de servidor somente de cache-
ção.

Escrevendo o arquivos de Mestre

Exemplo 6,10, Exemplo 6.11, Exemplo 6,12,e Exemplo 6,13 give arquivos de exemplo para um servidor de nome no BREW Ery, localizado na *vlager*. Devido à natureza da rede de discussão (uma única LAN), o exemplo é bastante simples-
para a frente.

A *named.ca* arquivo de cache mostrada na Exemplo 6,10 shoregistros de amostra foi dica de um servidor de nomes raiz. Um

típico
arquivo em cache geralmente descreve sobre uma dúzia de servidores de nome. Você pode obter a lista atual de servidores de nome para o
domínio raiz usando o `nslookup` ferramenta descrita na próxima seção.[43]

Exemplo 6.10: A named.ca Arquivo

```
;
; / Var / named / named.ca     Cache de arquivo para a cervejaria.
;                Nós não estamos na Internet, de modo que não precisamos
;                todos os servidores raiz. Para ativar essas
;                registros, remova o ponto e vírgula.
;
;.                          3600000  EM  NS    A.root SERVERS.NET.
; A.root SERVERS.NET.       3600000      A     198.41.0.4
;.                          3600000      NS    B.ROOT SERVERS.NET.
; B.ROOT SERVERS.NET.       3600000      A     128.9.0.107
;.                          3600000      NS    C.ROOT SERVERS.NET.
; C.ROOT SERVERS.NET.       3600000      A     192.33.4.12
;.                          3600000      NS    D.ROOT SERVERS.NET.
; D.ROOT SERVERS.NET.       3600000      A     128.8.10.90
;.                          3600000      NS    E.ROOT SERVERS.NET.
; E.ROOT SERVERS.NET.       3600000      A     192.203.230.10
;.                          3600000      NS    F.ROOT SERVERS.NET.
; F.ROOT SERVERS.NET.       3600000      A     192.5.5.241
;.                          3600000      NS    G.ROOT SERVERS.NET.
; G.ROOT SERVERS.NET.       3600000      A     192.112.36.4
;.                          3600000      NS    H.ROOT SERVERS.NET.
; H.ROOT SERVERS.NET.       3600000      A     128.63.2.53
;.                          3600000      NS    I.ROOT SERVERS.NET.
; I.ROOT SERVERS.NET.       3600000      A     192.36.148.17
;.                          3600000      NS    J.root SERVERS.NET.
; J.root SERVERS.NET.       3600000      A     198.41.0.10
;.                          3600000      NS    K.ROOT SERVERS.NET.
; K.ROOT SERVERS.NET.       3600000      A     193.0.14.129
;.                          3600000      NS    L.ROOT SERVERS.NET.
; L.ROOT SERVERS.NET.       3600000      A     198.32.64.12
;.                          3600000      NS    M.ROOT SERVERS.NET.
; M.ROOT SERVERS.NET.       3600000      A     202.12.27.33
;
```

43. Observe que você pode não consulta o servidor de nome para os servidores raiz, se você tiver um servidor instalado dicas de raiz. Para escapar desse

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

dilema,

você pode fazer `nslookup` usar um servidor de nome diferente, ou usar o arquivo de exemplo Exemplo 6,10 como ponto de partida e, em seguida ob-manter a lista completa dos servidores válido.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Exemplo 6.11: A named.hosts Arquivo

```
;                               hospeda no local da cervejaria
; / Var / named / named.hosts    Origin é vbrew.com
;
;
@               EM  SOA   vlager.vbrew.com. janet.vbrew.com. (
                          2000012601; serial
                          86400      ; Actualização: uma vez por dia
                          3600       ; Repetir: uma hora
                          3600000    ; Expirar: 42 dias
                          604800     ; Mínima: 1 semana
                          )
                EM  NS    vlager.vbrew.com.
;
; Correio local é distribuído em vlager
                EM  MX    10 vlager
;
; Endereço de loopback
localhost.      EM  A     127.0.0.1
;
; Ethernet Cervejaria
Virtual
vlager          EM  A     172.16.1.1
vlager-if1      EM  vlager CNAME
; Vlager também é servidor de notícias
notícias        EM  vlager CNAME
vstout          EM  A     172.16.1.2
Vale            EM  A     172.16.1.3
;
; Ethernet Adega Virtual
vlager-if2      EM  A     172.16.2.1
vbardolino      EM  A     172.16.2.2
vchianti        EM  A     172.16.2.3
vbeaujolais     EM  A     172.16.2.4
;
; Virtual Espíritos (filial), Ethernet
vbourbon        EM  A     172.16.3.1
vbourbon-if1    EM  vbourbon CNAME
```

Exemplo 6.12: O Arquivo named.local

```
                                Reverse mapeamento de 127.0.0
;                               Origin é 0.0.127.in addr.arpa.
; / Var / named / named.local
;
;
@             EM  SOA   vlager.vbrew.com. joe.vbrew.com. (
                        1          ; Série
                        360000     ; Atualização: 100 horas
                        3600       ; Repetir: uma hora
                        3600000    ; Expirar: 42 dias
                        360000     ; Mínima: 100 horas
                        )
              EM  NS    vlager.vbrew.com.
1             EM  PTR   localhost.
                                   ;
```

Exemplo 6.13: A named.rev

Arquivo

```
;
; / Var / named / named.rev
;
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
                                Reverse mapeamento dos nossos endereços de IP
                                 Origin é 16.172.in addr.arpa.

@               EM  SOA   vlager.vbrew.com. joe.vbrew.com. (
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
                        16          ; Série
                        86400       ; Actualização: uma vez por dia
                        3600        ; Repetir: uma hora
                        3600000     ; Expirar: 42 dias
                        604800      ; Mínima: 1 semana
                        )
              EM  NS    vlager.vbrew.com.
; Cervejaria
1.1           EM  PTR   vlager.vbrew.com.
2.1           EM  PTR   vstout.vbrew.com.
3.1           EM  PTR   vale.vbrew.com.
; Adega
1.2           EM  PTR   vlager-if2.vbrew.com.
2.2           EM  PTR   vbardolino.vbrew.com.
3.2           EM  PTR   vchianti.vbrew.com.
4.2           EM  PTR   vbeaujolais.vbrew.com.
```

Verificando a Instalação de Servidor de Nomes

`nslookup` é uma ótima ferramenta para verificar o funcionamento da sua configuração do servidor de nome. Pode ser usado

tanto interativamente

com instruções e como um único comando com saída imediata. Neste último caso, basta invocá-la como:

```
$ nslookup
hostname
```

`nslookup` consulta o servidor de nome especificado no *resolv.conf* para *hostname*. (Se este arquivo nomes mais do que um servidor, `nslookup` escolhe um aleatoriamente.)

O modo interativo, no entanto, é muito mais emocionante. Além de observar os hosts individuais, você pode consultar qualquer tipo de registro de DNS e transferir as informações de zona para um domínio inteiro.

Quando chamado sem um argumento, `nslookup` exibe o nome do servidor que ele usa e entra em modo interativo. Em o > prompt, você pode digitar qualquer nome de domínio que você deseja consultar. Por padrão, ele pergunta para a classe de registros, os

contendo o endereço IP relativo ao nome de domínio.

Você pode procurar por tipos de registro de emissão:

```
> tipo de conjunto =tipo
```

em que *tipo* é um dos nomes de registro de recurso descrito anteriormente, ou qualquer.

Você pode ter a seguinte `nslookup` sessão:

```
$ nslookup
Servidor Padrão: tao.linux.org.au
Endereço: 203.41.101.121

> metalab.unc.edu
Servidor:   tao.linux.org.au
Endereço: 203.41.101.121

Nome:    metalab.unc.edu
Endereço: 152.2.254.81
```

A saída exibe primeiro o servidor DNS que está sendo consultado e, em seguida o resultado da consulta.

Se você tentar a consulta para um nome que não tem um endereço IP associado a ele, mas outros registros foram encontrados no

DNS

banco de dados, `nslookup` retorna com uma mensagem de erro dizendo "`Nenhum tipo de registros encontrados`. "No entanto, você

pode fazê-lo de consulta para outros registros de tipo A, emitindo o `definir o tipo` comando. Para obter o registro de SOA *unc.edu*, Você faria:

```
> unc.edu
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
Servidor:   tao.linux.org.au
Endereço: 203.41.101.121
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
*** Sem endereço (A) os registros disponíveis para unc.edu
> tipo de conjunto = SOA
> unc.edu
Servidor:   tao.linux.org.au
Endereço: 203.41.101.121

unc.edu
        origin = ns.unc.edu
        addr mail = reg.ns.unc.edu host
        serial = 1998111011
        refresh = 14400 (4H)
        tentar novamente      = 3600 (1H)
        expirar = 1209600 (2W)
        TTL mínimo = 86400 (1D)
unc.edu nome do servidor = ns2.unc.edu
unc.edu servidor nome = ncnoc.ncren.net
unc.edu nome do servidor = ns.unc.edu
ns2.unc.edu     endereço na internet = 152.2.253.100
endereço na Internet ncnoc.ncren.net = 192.101.21.1
endereço na Internet ncnoc.ncren.net = 128.109.193.1
ns.unc.edu      endereço na internet = 152.2.21.1
```

De forma semelhante, você pode consultar registros MX:

```
> tipo de conjunto = MX
> unc.edu
Servidor:   tao.linux.org.au
Endereço: 203.41.101.121

preferência unc.edu = 0, o cambista mail = conga.oit.unc.edu
preferência unc.edu = 10, o cambista mail = imsety.oit.unc.edu
unc.edu nome do servidor = ns.unc.edu
unc.edu nome do servidor = ns2.unc.edu
unc.edu servidor nome = ncnoc.ncren.net
conga.oit.unc.edu       endereço na internet = 152.2.22.21
imsety.oit.unc.edu      endereço na internet = 152.2.21.99
ns.unc.edu      endereço na internet = 152.2.21.1
ns2.unc.edu     endereço na internet = 152.2.253.100
endereço na Internet ncnoc.ncren.net = 192.101.21.1
endereço na Internet ncnoc.ncren.net = 128.109.193.1
```

Usando um tipo de qualquer retorna todos os registros de recursos associados a um determinado nome.

A aplicação prática da `nslookup`, Além de depuração, é obter a lista atual de servidores de nomes raiz. Você pode obter essa lista por meio de consulta para todos os registros NS associadas ao domínio root:

```
> tipo de conjunto = NS
> .
Servidor:   tao.linux.org.au
Endereço: 203.41.101.121

resposta não oficial:
(Root)  nome do servidor = a.root-SERVERS.NET
(Root)  nome do servidor = H.ROOT-SERVERS.NET
(Root)  nome do servidor = B.ROOT-SERVERS.NET
(Root)  nome do servidor = C.ROOT-SERVERS.NET
(Root)  nome do servidor = D.ROOT-SERVERS.NET
(Root)  nome do servidor = E.ROOT-SERVERS.NET
(Root)  nome do servidor = I.ROOT-SERVERS.NET
(Root)  nome do servidor = F.ROOT-SERVERS.NET
(Root)  nome do servidor = G.ROOT-SERVERS.NET
(Root)  nome do servidor = j.root-SERVERS.NET
(Root)  nome do servidor = K.ROOT-SERVERS.NET
(Root)  nome do servidor = L.ROOT-SERVERS.NET
(Root)  nome do servidor = M.ROOT-SERVERS.NET
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
Autorizadas respostas podem ser encontradas a partir de:
A.root-SERVERS.NET      endereço na internet = 198.41.0.4
H.ROOT-SERVERS.NET      endereço na internet = 128.63.2.53
B.ROOT-SERVERS.NET      endereço na internet = 128.9.0.107
C.ROOT-SERVERS.NET      endereço na internet = 192.33.4.12
D.ROOT-SERVERS.NET      endereço na internet = 128.8.10.90
E.ROOT-SERVERS.NET      endereço na internet = 192.203.230.10
I.ROOT-SERVERS.NET      endereço na internet = 192.36.148.17
F.ROOT-SERVERS.NET      endereço na internet = 192.5.5.241
G.ROOT-SERVERS.NET      endereço na internet = 192.112.36.4
J.root-SERVERS.NET      endereço na internet = 198.41.0.10
K.ROOT-SERVERS.NET      endereço na internet = 193.0.14.129
L.ROOT-SERVERS.NET      endereço na internet = 198.32.64.12
M.ROOT-SERVERS.NET      endereço na internet = 202.12.27.33
```

Para ver o conjunto completo de comandos disponíveis, utilize o `Ajuda` comando em `nslookup`.

Outras ferramentas úteis

Existem algumas ferramentas que podem ajudá-lo com suas tarefas como um administrador de BIND. Iremos descrever

brevemente dois dos
-los aqui. Consulte a documentação que vem com essas ferramentas para obter mais informações sobre como usar
elas.

`hostcvt` ajuda com a sua configuração BIND inicial, convertendo o */ Etc / hosts* arquivo em arquivos mestre para `nomeado`. Ele gera tanto para frente (A) e mapeamento reverso (PTR) entradas, e cuida de aliases. De
É claro que não vai fazer todo o trabalho para você, como você ainda pode querer ajustar os valores de tempo limite no registro SOA, por
exemplo, ou adicionar registros MX. Ainda assim, ele pode ajudar você a economizar um pouco aspirinas. `hostcvt` faz parte da fonte de BIND,
mas também pode ser encontrado como um pacote autônomo em alguns servidores de FTP Linux.

Após configurar o servidor de nomes, você pode querer testar a configuração. Algumas boas ferramentas que fazem este trabalho muito mais simples: o primeiro é chamado `dnswalk`, Que é um pacote baseado em Perl. O segundo é chamado `nslint`. Eles tanto passear com o banco de dados DNS procurando erros mais comuns e verificar que a informação que eles encontram é consis-
barraca. Duas outras ferramentas úteis são `host` e `cavar`, Que são DNS objetivo geral do banco de dados ferramentas de consulta. Você pode
usar essas ferramentas para inspecionar manualmente e diagnosticar as entradas de DNS banco de dados.

Essas ferramentas são susceptíveis de ser disponibilizados em formato pré-embalados. `dnswalk` e `nslint` estão disponíveis na fonte http://www.visi.com/ ~ barr / dnswalk / umdftp://ftp.ee.lbl.gov/nslint.tar.Z.A `host` e `cavar` códigos-fonte pode ser encontrada em ftp://ftp.nikhef.nl/pub/network/ umdftp://ftp.is.co.za/networking/ip/dns/dig/.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 7 - Serial Line IP

protocolos de pacotes, como IP ou IPX invocar o host receptor saber onde o início eo fim de cada pacote estão em o fluxo de dados. O mecanismo usado para marcar e detectar o início eo término dos pacotes é chamado *delimitação*. A protocolo Ethernet gere este mecanismo em ambiente LAN, e os protocolos SLIP e PPP gerenciá-lo para as linhas de comunicação serial.

O custo relativamente baixo de modems de conexão discada de baixa velocidade e circuitos telefônicos fez a linha serial IP protocolos imensamente popular, especialmente para fornecer conectividade para os usuários finais da Internet. O novo hardware cessária para executar SLIP ou PPP é simples e facilmente disponível. Tudo o que é necessário é um modem e uma porta serial equipado com um buffer FIFO.

O protocolo SLIP é muito simples de implementar e ao mesmo tempo era o mais comum dos dois. Hoje, quase todo mundo usa o protocolo PPP. O protocolo PPP adiciona uma série de recursos sofisticados que contribuem para sua popularidade, hoje e veremos o mais importante destes últimos.

O Linux suporta os drivers do kernel baseado tanto para SLIP e PPP. Os motoristas foram ambas em torno de algum tempo e são estáveis e confiáveis. Neste capítulo e no próximo, vamos discutir os dois protocolos e como configurá-los.

Requisitos Gerais

Para usar SLIP ou PPP, você tem que configurar alguns recursos básicos de rede como descrito nos capítulos anteriores. Você deve configurar a interface de loopback e configurar o resolvedor de nomes. Ao se conectar a Internet, você vai querer usar DNS. Suas opções aqui são as mesmas do PPP: você pode executar consultas DNS em sua ligação em série, configurando o seu endereço de Internet Service Provider IP em sua */ Etc / resolv.conf* arquivo, ou configura um servidor de nomes somente de cache, como descrito em "Configuração Caching-somente com o nome" no Capítulo 6, *"Nome Serviço e configuração do resolvedor*".

SLIP Operação

servidores dial-up IP freqüentemente oferecem serviços SLIP por meio de contas especiais de usuário. Depois de fazer login para tal accontar, você não está descartado para o reservatório comum, em vez disso, um script shell ou programa é executado, que permite a driver SLIP servidor para a linha serial e configura a interface de rede apropriada. Então você tem que fazer o mesmo em sua extremidade do link.

Em alguns sistemas operacionais, o motorista SLIP é um programa de espaço do usuário; no Linux, é parte do kernel, o que torna muito mais rápido. Esta velocidade, exige no entanto que a linha serial ser convertido para o modo de SLIP explicitamente. Esta conversão é feita por meio de uma disciplina especial tty linha, SLIPDISC. Enquanto o tty está em linha normal dis- Acostumados à disciplina rigorosa (DISC0), dados que troca apenas com os processos de usuário, usando o normal *read (2)* e *write (2)* chamadas, e os driver SLIP é incapaz de escrever ou ler a partir do terminal. Em SLIPDISC, os papéis se inverteram: agora qualquer utilizador de espaço processos são impedidos de gravar ou ler a partir do tty, enquanto todos os dados que chegam através da porta serial é passados diretamente para o driver SLIP.

O motorista SLIP si compreende uma série de variações sobre o protocolo SLIP. Além de SLIP ordinário, também entende CSLIP, que realiza a chamada Van compressão do cabeçalho Jacobson (descrito na RFC-1144) em pacotes IP de saída. Esta compressão aumenta a taxa de transferência para sessões interativas visivelmente. Não também versões de seis bits para cada um destes protocolos.

Uma maneira simples de converter uma linha serial SLIP modo é usando o `slattach` ferramenta. Suponha que você tenha o seu modem */ Dev/ttyS3* e ter entrado para o servidor SLIP com êxito. Você irá então executar:

```
# slattach / dev/ttyS3 &
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Esta ferramenta muda a disciplina da linha de *ttyS3* para `SLIPDISC` e atribui-la a uma das inter-rede SLIP faces. Se esta é sua primeira ligação SLIP ativo, a linha será anexado ao *sl0*, A segunda será anexada ao *sl1*E assim por diante. Os kernels atuais suportam um máximo padrão de 256 ligações simultâneas SLIP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A disciplina de linha padrão escolhido pelo `slattach` é CSLIP. Você pode escolher qualquer outra disciplina com o *-P* switch. Para usar SLIP normal (sem compressão), você usa:

```
# slattach p-slip / dev/ttyS3 &
```

As disciplinas disponíveis estão listados na Tabela 7.1.Um especial pseudo-disciplina está disponível chamado `adaptativo`, que faz com que o kernel detecta automaticamente qual o tipo de encapsulamento SLIP está sendo usado por controle remoto finais.

Tabela 7.1: Disciplinas Linux Slip-Line

Descrição Disclipline	
escorregar	encapsulamento SLIP tradicional.
cslip	SLIP encapsulamento com Van compressão do cabeçalho Jacobsen.
slip6	SLIP encapsulamento com a codificação de seis bits. O método de codificação é semelhante ao utilizado por o `uuencode` comando, e faz com que o datagrama SLIP para ser convertido em impressão caracteres ASCII. Esta conversão é útil quando você não tem uma ligação de série que é de oito pouco limpo.
cslip6	SLIP encapsulamento com Van Jacobsen cabeçalho compressão e codificação de seis bits.
adaptativo	Esta não é uma disciplina da linha real, ao contrário, faz com que o kernel para tentar identificar a linha disciplina que está sendo utilizado pela máquina remota e igualá-la.

Observe que você deve usar o mesmo encapsulamento como seu par. Por exemplo, se *primavera* CSLIP usa, você também tem fazê-lo. Se sua conexão SLIP não funcionar, a primeira coisa que você deve fazer é garantir que ambas as extremidades da ligação
concordo em se usar a compressão do cabeçalho ou não. Se você não tiver certeza que o host remoto está usando, tente Configur-
ing seu host para o deslizamento de adaptação. O kernel pode descobrir o tipo certo para você.

`slattach` permite ativar não só SLIP, mas outros protocolos que utilizam a linha de série, como PPP ou KISS (outro protocolo utilizado por pessoas de rádio amador). Fazer isso não é comum, embora, e existem ferramentas disponíveis para melhor
suportem estes protocolos. Para mais informações, consulte o *slattach (8)* manual de página.

Depois de virar a linha para o driver SLIP, você deve configurar a interface de rede. Mais uma vez, você faz isso usando o padrão `ifconfig` e `rota` comandos. Suponha que temos marcado um servidor nomeado *primavera* a partir de *vlager*. Em vlager você deve executar:

```
# ifconfig sl0 cowslip pointopoint deslizamento vlager-
# route add cowslip
# route add default gw cowslip
```

O primeiro comando configura a interface como um link ponto-a-ponto para *primavera*, Enquanto o segundo e terceiro adicionar o
rota para *primavera* e via o padrão, usando *primavera* como um gateway.

Duas coisas são dignas de nota sobre o `ifconfig` invocação: O *pointopoint* opção que especifica o endereço do fim de um link ponto-a-ponto e nosso uso de *vlager-derrapante* como o endereço da interface SLIP local.

Já mencionamos que você pode usar o mesmo endereço atribuído ao *vlager*"Interface Ethernet s para o seu SLIP link, também. Neste caso, *vlager-derrapante* só poderia ser outro alias para o endereço *172.16.1.1*. No entanto, também é pos-
É possível que você tem que usar um endereço completamente diferente para o seu link SLIP. Um desses casos é quando sua rede

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

utiliza um endereço de rede IP privativos, como a Cervejaria faz. Voltaremos a este cenário em maior detalhe no próxima seção.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Para o restante deste capítulo, vamos usar sempre *vlager-derrapante* remeter para o endereço do local SLIP

inter-
rosto.

Ao derrubar a ligação SLIP, você deve primeiro remover todas as rotas através de *primavera* usando `rota` com o *del* opção, e depois faça a interface para baixo, e enviar `slattach` o sinal de desligar. O que você deve desligar o modem usando o seu programa de terminal novamente:

```
# rota padrão del
# cowslip rota del
# ifconfig sl0 baixo
# kill-HUP 516
```

Note-se que o *516* deve ser substituído com o ID do processo (como mostrado na saída do `ps ax`) Do `slattach` comandos que controlam o dispositivo de deslizamento que deseja derrubar.

Lidar com a Private IP Redes

Você vai se lembrar do capítulo 5, *Configurando Redes TCP / IP*, Que a Cervejaria Virtual tem uma Ethernet rede baseada em IP usando números de rede não registrados, que são reservados apenas para uso interno. Pacotes para ou a partir uma dessas redes não são roteados na Internet, se tivéssemos *vlager* discagem em *primavera* e agir como um roteador para a rede Cervejaria Virtual hosts dentro da rede da cervejaria não podia falar com hosts da Internet real diretamente porque seus pacotes seria abandonada em silêncio o primeiro roteador principal.

Para contornar esse dilema, vamos configurar *vlager* para atuar como uma espécie de rampa de lançamento para acessar Internet serviços. Para o mundo exterior, ele vai se apresentar como um host da Internet normal SLIP conectado com um IP registrado endereço (provavelmente atribuído pelo provedor de rede em execução *primavera*). Qualquer um logado para *vlager* pode usar o texto
programas baseados como `ftp`,`telnet`, Ou mesmo `lince` fazer uso da Internet. Qualquer pessoa na Cervejaria Virtual LAN pode, portanto, telnet e login para *vlager* e usar os programas lá. Para algumas aplicações, pode haver soluções que evitem acessar a *vlager*. Para usuários de WWW, por exemplo, podemos executar uma chamada *servidor proxy* em *vlager*, Que todos os pedidos de retransmissão de seus usuários para os respectivos servidores.

Tendo para fazer login no *vlager* fazer uso da Internet é um pouco desajeitado. Mas, além de eliminar a papelada (E custos) de registro de uma rede IP, que tem a vantagem de ir bem com uma configuração de firewall. Fogo-paredes são pessoas dedicadas usado para fornecer acesso limitado à Internet para os usuários em sua rede local sem expor os hosts internos de ataques à rede do mundo exterior. Simples configuração de firewall é coberto em mais detalhes no Capítulo 9, *Firewall TCP / IP*. No capítulo 11, *IP Masquerade e Network Address Translation*, Vamos discutir um recurso do Linux chamado "IP Masquerade", que proporciona uma poderosa alternativa para os servidores proxy.

Suponha que a cervejaria tenha sido atribuído um endereço IP *192.168.5.74* de acesso SLIP. Tudo que você precisa fazer para perceber que a configuração que descrevemos acima é de introduzir este endereço na sua */ Etc / hosts* arquivo, nomeando-*vlager-derrapante*. A
Procedimento para colocar o link SLIP permanece inalterada.

Usando mergulho

Agora que foi bastante simples. No entanto, você pode querer automatizar os passos descritos anteriormente. Seria ser muito melhor ter um comando simples que executa todos os passos necessários para abrir o dispositivo serial, causa o modem para discar para o provedor, login, permitir que a disciplina da linha SLIP e configurar a interface de rede. Este é o que o `mergulho` comando é para.

`mergulho` meios *Discagem IP*. Ela foi escrita por Fred Van Kempen e foi corrigido fortemente por uma série de pessoas. Hoje existe uma tensão que é usado por quase todos: Versão `dip337p-uri`, Que está incluído com a maioria das distribuições Linux modernas, ou está disponível a partir do *metalab.unc.edu* FTP arquivo.

`mergulho` fornece um interpretador para uma linguagem de script simples que pode manipular o modem para você, converter a

linha
para o modo de SLIP e configurar as interfaces. A linguagem de script é poderoso o suficiente para atender a maioria das configurações.

Para ser capaz de configurar a interface SLIP, `mergulho` requer privilégios de root. Agora vai ser tentador fazer `mergulho`

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

setuid para *root* de modo que todos os usuários podem discar para algum servidor SLIP sem ter de dar-lhes acesso root. Isso é muito
perigosas, embora, porque a criação de interfaces falso e rotas padrão com `mergulho` pode perturbar o seu encaminhamento em
rede. Ainda pior, essa ação seria dar o seu poder os usuários se conectem *qualquer* SLIP servidor e perigo-lançamento

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

ous ataques em sua rede. Se você quiser permitir que seus usuários para disparar uma conexão SLIP, escrever pequeno wrapper programas para cada servidor SLIP em perspectiva e ter esses invólucros invocar `mergulho` com o roteiro específico que estabelece a conexão. programas wrapper cuidadosamente escrita pode ser feita com segurança setuid para *root*.[44] Um alternativa, a abordagem mais flexível para dar aos usuários acesso a raiz confiável `mergulho` usando um programa como `sudo`.

Um script de exemplo

Suponha que o host para o qual nós fazemos nossa conexão SLIP é *primavera*, E que nós escrevemos um roteiro para `mergulho` para executar chamada *cowslip.dip* que torna a nossa ligação. Nós invocamos `mergulho` com o nome do script como argumento:

```
# mergulho cowslip.dip
DIP: Dialup IP Driver versão 3.3.7 Protocolo (12/13/93)
Escrito por Fred N. van Kempen, MicroWalt Corporation.
ligado ao cowslip.moo.com com addr 192.168.5.74
#
```

O script em si é mostrada na Exemplo 7.1.

Exemplo 7.1: Um mergulho Script de exemplo

```
# Exemplo de script de mergulho para marcação de prímula
# Defina o nome do local e remoto e endereço
        receber US $ local vlager-derrapante
        obter cowslip $ remota
        porta ttyS3                # Escolha uma porta serial
        velocidade de 38400      # Definir a velocidade máxima de
        HAYES modem              # Defina o tipo de modem
        reset                    # Modem reset e tty
        resplendor               # Expulsar resposta do modem
# Prepare-se para a marcação.
        envie r \ ATQ0V1E1X1
        esperar 2 OK
        se $ errlvl! = Error GoTo 0
        dial 41988
        se $ errlvl! = Error GoTo 0
        esperar CONNECT 60
        se $ errlvl! = Error GoTo 0
# Ok, estamos conectados agora
        sleep 3
        envie r \ \ n \ r \ n
        esperar ogin: 10
        se $ errlvl! = Error GoTo 0
        enviar Svlager \ n
        esperar ssword: 5
        se $ errlvl! = Error GoTo 0
        enviar KnockKnock \ n
        esperar correr 30
        se $ errlvl! = Error GoTo 0
# Temos logado, eo lado remoto estiver iniciando SLIP.
        Conectado a impressão remota $ $ com o endereço rmtip
        padrão                   # Fazer esta ligação nossa rota padrão
        modo SLIP                # Vamos para o modo de SLIP, também
# Cair em caso de erro
erro:
        SLIP imprimir $ remoto falhou.
```

Depois de se conectar *primavera* e permitindo SLIP, `mergulho` vai destacar a partir do terminal e vá para o fundo. Você pode então começar a utilizar os serviços de rede normal no link SLIP. Para terminar a ligação, simplesmente invocar `mergulho` com o *-K* opção. Isso envia um sinal de desligar para `mergulho`, Usando a identificação do processo `mergulho` registros em */ Etc / dip.pid*:

```
# dip-k
```

[44] `diplogin` deve ser executado como setuid para *root*Também. Consulte a seção no final deste capítulo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Em `mergulho`É a linguagem de scripts, palavras-chave prefixados com um dólar símbolo nomes de variáveis denotam. `mergulho` tem uma prede-
multado conjunto de variáveis, que serão listados abaixo. *$ Remota* e *$ Local*, Por exemplo, contêm os nomes de host do hosts remotos e locais envolvidos na ligação SLIP.

As duas primeiras instruções no script de exemplo são `obter` comandos, que é `mergulho`É maneira de definir uma variável.

Aqui, o
hosts locais e remotos são definidos para *vlager* e *primavera*, Respectivamente.

Os próximos cinco declarações configurar o terminal da linha e do modem. *reset* envia uma seqüência de reset ao modem. A próxima declaração libera a resposta do modem para que a sessão de bate-papo na próximas linhas funciona corretamente. Este chat é bastante simples: ele simplesmente disca 41988, o número de telefone *primavera*E registros na conta *Svlager* usando a senha *KnockKnock*. A *esperar* comando faz `mergulho` aguardar a string dada no ar sua primeira fesa, o número dado como seu segundo argumento faz com que o tempo de espera para fora depois que segundo muitos, se não como
string é recebida. A *se* comandos entremeadas no processo de verificação de login que nenhum erro ocorreu durante a executing o comando.

Os comandos executados após o final login são *padrão*, Que faz a ligação SLIP a rota padrão para todos hospedeiros, e *Modo*, Que habilita o modo SLIP na linha e configura a interface ea tabela de roteamento para você.

Uma referência mergulho

Nesta seção, vamos dar uma referência para a maioria dos `mergulho`'S comandos. Você pode obter uma visão geral de todas as

forças com-
mandos que prevê, invocando `mergulho` em modo de teste e entrar no *Ajuda* comando. Para saber mais sobre a sintaxe de uma comando, você pode digitá-lo sem argumentos. Lembre-se que isso não funciona com os comandos que levam sem argumentos. O exemplo a seguir ilustra a *Ajuda* comando:

```
# dip-t
DIP: Dialup IP Driver Protocolo 3.3.7p versão uri (25 de dezembro 96)
Escrito por Fred N. van Kempen, MicroWalt Corporation.
3.3.7p versão Debian-2 (debian).

DIP> Ajuda
DIP sabe sobre os seguintes comandos:

        bip             bootp           quebrar         chatkey         config
        databits        dezembro        padrão          dial            echo
        resplendor      obter           goto            Ajuda           se
        inc             init            Modo            modem           netmask
        OnExit          paridade        senha           proxyarp        impressão
        psend           porto           parar           reset           securidfixed
        SecurID         enviar          shell           skey            sono
        velocidade      stopbits        prazo           timeout         esperar

DIP> echo
Uso: echo on | off
DIP>
```

Durante a seção a seguir, exemplos que mostram o `DIP>` prompt mostrar como inserir um comando em teste modo de produção eo que ela produz. Exemplos sem este aviso deve ser tomado como trechos de script.

O modem comandos

`mergulho` fornece um número de comandos que configuram a sua linha serial e modem. Alguns deles são óbvios, como *porto*, Que seleciona uma porta serial, e *velocidade*,*databits*,*stopbits*E *paridade*, Que definiu a linha comum parâmetros. A *modem* comando seleciona um tipo de modem. Atualmente, o tipo só é suportada *HAYES* (Capitalização necessário). Você tem que fornecer `mergulho` com um tipo de modem, ou então ele irá recusar a execução de *dial* e *reset*
comandos. A *reset* comando envia uma seqüência de reset ao modem, a string utilizada depende do tipo de modem selecionado. Para modems Hayes-compatible, essa seqüência é *ATZ*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A *resplendor* código pode ser usado para lavar todas as respostas do modem enviou até agora. Caso contrário, um script de chat acompanhamento
ing *reset* pode ser confuso porque ele lê o *OK* respostas dos comandos anteriores.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A *init* comando seleciona uma seqüência de inicialização a serem passados para o modem antes de discar. O padrão para Hayes modems é "*ATE0 Q0 V1 X1*", Que gira em torno de eco de comandos e códigos de resultado de longo e seleciona cegos discagem (não verificação de tom de discagem). modems modernos têm uma boa configuração padrão de fábrica, de modo que este é um pouco
desnecessária, mas não faz mal nenhum.

A *dial* comando envia a seqüência de inicialização para o modem e disca o sistema remoto. O padrão de marcação comando para modems Hayes é *ATD*.

O comando echo

A *echo* comando serve como uma ajuda de depuração. Chamada *eco em* faz `mergulho` echo para o console tudo o que envia para o dispositivo serial. Isso pode ser desligada novamente chamando *echo off*.

`mergulho` também permite que você sair do modo de script temporariamente e entrar no modo terminal. Neste modo, você pode usar `mergulho`
como qualquer outro programa de terminal normal, escrevendo os caracteres que você digitar a linha serial, ler os dados do linha de série, e exibindo os personagens. Para sair deste modo, digite Ctrl-].

O comando get

A *obter* comando é `mergulho`É maneira de definir uma variável. A forma mais simples é definir uma variável como uma constante, assim como nós
fez em *cowslip.dip*. Você pode, entretanto, também alerta o usuário para a entrada, especificando a palavra-chave *perguntar* em vez de um
valor:

```
DIP> receber US $ perguntar local
Digite o valor em R $ local: _
```

Um terceiro método consiste em obter o valor a partir do host remoto. Estranho como parece à primeira vista, isso é muito útil em alguns dos casos. Alguns servidores SLIP não vai permitir que você use seu próprio endereço IP no link SLIP, mas sim atribuir Você é um de um pool de endereços sempre que você disca, imprimir alguma mensagem que informa sobre a ad-
vestido que você tenha sido atribuído. Se a mensagem é algo como "`Seu endereço: 192.168.5.74`", O seguinte trecho de `mergulho` código iria deixá-lo pegar o endereço:

```
# Acabamento login
esperar endereço: 10
receber US $ locip remoto
```

O comando de impressão

Este é o comando utilizado para echo de texto para o console no qual `mergulho` foi iniciado. Qualquer um dos `mergulho`'S variáveis podem
ser usado em comandos de impressão. Está aqui um exemplo:

```
DIP> porta de impressão Usando $ $ porta a uma velocidade de velocidade
Usando a porta ttyS3 na velocidade 38400
```

Os nomes de variáveis

`mergulho` só compreende um conjunto predefinido de variáveis. Um nome de variável sempre começa com um símbolo de dólar e
deve ser escrito em letras minúsculas.

A *$ Local* e *$ Locip* variáveis conter o nome do host local e endereço IP. Ao armazenar o host-canônica nome em *$ Local*,`mergulho` automaticamente tentará resolver o hostname para um endereço IP e para armazená-lo no *$ Locip* variável. Um processo semelhante, mas inverso ocorre quando você atribui um endereço IP para o *$ Locip* variável; `mergulho` tentará executar uma pesquisa inversa para identificar o nome do host e armazená-lo no *$ Local* variável.

A *$ Remota* e *$ Rmtip* variáveis operam da mesma forma para o nome do host remoto e endereço. *$ Mtu* contém o valor da MTU para a conexão.

Essas cinco variáveis são os únicos que podem ser atribuídos valores diretamente usando o *obter* comando. Um certo número de outras variáveis são definidos como um resultado da configuração de comandos com o mesmo nome, mas pode ser usado em

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

impressão declarações, estas variáveis são *$ Modem*,*$ Porta*E *$ Velocidade*.

$ ErrlvI é a variável através do qual você pode acessar o resultado do último comando executado. Um nível de erro de 0 indica sucesso, enquanto um valor diferente de zero indica um erro.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Os comandos if e goto

A *se* comando é um ramo condicional, ao invés de uma programação completa *se* declaração. Sua sintaxe é:

`se` *Número op var* `goto` *etiqueta*

A expressão deve ser uma simples comparação entre uma das variáveis *$ Errlvl*,*$ Locip*E *$ Rmtip.var* deve ser um número inteiro, o operador *op* pode ser um dos ==,! =,<,>,<=E > =.

A *goto* comando faz com que a execução do script continuar na linha seguinte que ostentam a *etiqueta*. A rótulo deve ser a primeira palavra na linha e deve ser seguido imediatamente por uma vírgula.

enviar, esperar, e dormir

Estes comandos ajudar a implementar um chat simples scripts `mergulho`. A *enviar* comando emite os seus argumentos para o linha serial. Ele não suporta variáveis, mas compreende todas as seqüências de caracteres de estilo C barra invertida, como *\ N* para
nova linha e *\ B* de retrocesso. O til (~) pode ser usado como uma abreviação para retorno de carro / newline.

A *esperar* leva uma palavra de comando como um argumento e irá ler todas as entradas na linha serial até detectar uma se-seqüência de caracteres que correspondem a esta palavra. A palavra em si não podem conter espaços em branco. Opcionalmente, você pode dar
esperar um valor de tempo limite como um segundo argumento, se a palavra esperada não for recebido dentro desse segundo muitos, a
comando irá retornar com uma *$ Errlvl* valor de 1. Este comando é usado para detectar login e outros avisos.

A *sono* comando pode ser utilizado para esperar por um determinado período de tempo, por exemplo, esperar pacientemente por qualquer
seqüência de login para ser concluído. Novamente, o intervalo é especificado em segundos.

modo e padrão

Estes comandos são usados para lançar a linha serial para o modo de SLIP e configurar a interface.

A *Modo* comando é o último comando executado pelo `mergulho` antes de entrar em modo daemon. A menos que um erro ocorre, o comando não retornar.

Modo pega o nome do protocolo como argumento. `mergulho` atualmente reconhece *SLIP*,*CSLIP*,*SLIP6*,*CSLIP6*,*PPP*E *PRAZO* como nomes válidos. A versão atual do `mergulho` não entende SLIP adaptativa, no entanto.

Depois de ativar o modo SLIP na linha serial, `mergulho` executa `ifconfig` para configurar a interface como um ponto-a-link ponto, e invoca `rota` para definir a rota para o host remoto.

Se, além disso, o script executa o *padrão* comando antes *Modo*,`mergulho` cria uma rota padrão que aponta para a ligação SLIP.

Executando no modo de servidor

Configurando o seu cliente SLIP foi a parte mais difícil. Configurando o servidor deverá atuar como um servidor SLIP é muito mais fácil.

Há duas maneiras de configurar um servidor SLIP. Ambas as formas exigem que você configure um login por conta SLIP cliente. Suponha que você fornecer o serviço de SLIP para Arthur Dent na *dent.beta.com*. Você pode criar uma conta chamada *dente* adicionando a seguinte linha ao seu *passwd* arquivo:

```
dente: *: 501:60: conta Arthur Dent SLIP: / tmp: / usr / sbin / diplogin
```

Depois, você deve definir *dente*Está usando a senha `passwd` utilidade.

A `mergulho` comando pode ser usado no modo de servidor invocando-a como `diplogin`. Normalmente `diplogin` é um link para
`mergulho`. Seu arquivo de configuração principal é */ Etc / diphosts*, Que é onde você especifica o endereço IP de um usuário SLIP serão

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

atribuído quando ele ou ela disca dentro Alternativamente, você também pode usar o `sliplogin` comando, um instrumento derivado do BSD
apresentando um esquema de configuração mais flexível, que permite executar scripts shell sempre que um host se conecta e desconecta.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Quando nosso usuário SLIP *dente* loga, `mergulho` começa a funcionar como um servidor. Para descobrir se ele é de fato permitido usar SLIP, é
olha o nome de usuário */ Etc / diphosts*. Este arquivo de dados os direitos de acesso e conexão para cada parâmetro SLIP usuário. O formato geral para um */ Etc / diphosts* entrada é semelhante a:

```
# / Etc / diphosts
usuário:senha:rem-addr:LOC-addr:netmask:comentários:protocolo,MTU#
```

Cada um dos campos é descrito em Tabela 7.2.

Tabela 7.2: / etc / diphosts Campo Descrição

Campo	Descrição
`usuário`	O nome de usuário do usuário executando `mergulho` que esta entrada será aplicada.
senha senha de	Campo 2 do */ Etc / diphosts* arquivo é usado para adicionar uma camada extra de segurança baseados em a conexão. Você pode colocar uma senha de forma criptografada aqui (assim como no */ Etc / passwd*) e `diplogin` pedirá que o usuário digite a senha antes de permitir SLIP
	acesso. Note que esta senha é usada para além do normal `login`-Senha com base o usuário vai entrar.
`rem-addr`	O endereço que será atribuído à máquina remota. Esse endereço pode ser especificado ou como um host que será resolvido ou um endereço IP na notação "dotted quad.
`LOC-addr`	O endereço IP que será usado para este fim do link SLIP. Isso também pode ser especificado como um hostname resolúvel ou em formato dotted quad.
`netmask` essa	A máscara de rede que serão utilizados para fins de encaminhamento. Muitas pessoas ficam confusas com
	entrada. A máscara não se aplica à ligação SLIP em si, mas é usado em combinação com o `rem-addr` campo para produzir uma rota para o site remoto. A máscara deve ser a utilizados pela rede suportada pelo do host remoto.
`comentários` arquivo. É	Este campo é de formato livre de texto que você pode usar para ajudar a documentar o */ Etc / diphosts* não serve a nenhum outro propósito.
`protocolo`	Este campo é onde você especificar o protocolo ou a disciplina da linha que deseja aplicar ao presente conexão. As entradas válidas aqui são as mesmas válidas para o *-P* argumento para o `slattach` comando.
`MTU`	A unidade de transmissão máxima de que esta ligação irá transportar. Este campo descreve o maior datagrama que serão transmitidos através do link. Qualquer datagrama encaminhado para o dispositivo SLIP que é maior que a MTU serão fragmentados em datagramas não maior do que esse valor. Normalmente, a MTU está configurado de forma idêntica em ambas as extremidades do link.

Um exemplo de entrada para *dente* poderia ficar assim:

```
dente: vbrew.com: dent.beta.com 255.255.255.0: Arthur Dent: CSLIP, 296
```

Nosso exemplo dá aos nossos usuários *dente* acesso ao SLIP sem senha adicional. Ele será atribuído o IP endereço associado *dent.beta.com* com a máscara `255.255.255.0`. Sua rota padrão deve ser di-corrigidos para o endereço IP do *vbrew.com*, E ele irá utilizar o protocolo CSLIP com uma MTU de 296 bytes.

Quando *dente* loga, `diplogin` extrai as informações sobre ele a partir do *diphosts* arquivo. Se o segundo campo con-tem um valor, `diplogin` pedirá uma "senha de segurança externa." A sequência de caracteres digitados pelo usuário é en-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

crypted e comparada com a senha *diphosts*. Se eles não corresponderem, a tentativa de login é rejeitada. Se o campo de senha contém a seqüência *s / chave*E `mergulho` foi compilado com suporte chave S / S / Chave de autenticação será ter lugar. S / autenticação da chave está descrita na documentação que vem no `mergulho` origem do pacote.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Após um login bem sucedido, `diplogin` prossegue lançando a linha serial para o modo de CSLIP ou SLIP, e configura o interface e rota. Essa conexão permanece estabelecida até que o usuário se desconecta eo modem cai a linha. `diplogin` em seguida, retorna a linha para a disciplina de linha normal e sai.

`diplogin` requer privilégios de superusuário. Se você não tem `mergulho` execução setuid *root*, Você deve fazer `diplogin` uma cópia em separado do `mergulho` em vez de um simples link. `diplogin` pode então ser feita com segurança sem setuid
afetando a qualidade de `mergulho` em si.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 8 - O Protocolo Ponto-a-Ponto

Como SLIP, PPP é um protocolo utilizado para enviar datagramas através de uma conexão serial, porém, que aborda um casal das deficiências do SLIP. Primeiro, ele pode levar um grande número de protocolos e não é, portanto, limitada ao protocolo IP col. Ele fornece detecção de erros no link em si, enquanto SLIP aceita e envia datagramas corrompido enquanto a corrupção não ocorre no cabeçalho. Igualmente importante, ele permite que os lados se comunicando negociar opções, como o endereço IP eo tamanho máximo do datagrama em tempo de inicialização, e fornece a autorização do cliente. Este built-in permite a automação de negociação fiável do estabelecimento da conexão, enquanto a autenticação remove a necessidade de as contas de usuário desajeitado login que exige SLIP. Para cada uma destas capacidades, o PPP tem um separado
protocolo. Neste capítulo, fazemos uma breve cobrir esses blocos básicos de construção do PPP. Esta discussão de PPP está longe de ser
completa, se você quiser saber mais sobre o PPP, nós pedimos que você leia a especificação RFC e uma dúzia ou assim RFCs companheiro.[45] Há também um livro O'Reilly abrangente sobre o tema *Usando e gerenciamento da PPP*, Por Andrew dom.

Na parte inferior da PPP é o *High-Level Data Link Control* (HDLC) protocolo, que define os limites
em torno de quadros individuais PPP e proporciona um checksum de 16 bits.[46] Ao contrário do SLIP mais primitivo encapsulamento, um quadro PPP é capaz de manter pacotes de protocolos diferentes de IP, tais como IPX da Novell ou Appletalk. PPP realiza isso adicionando um campo de protocolo do frame HDLC básico que identifica o tipo de pacote transportado pelo quadro.

A *Protocolo de Controle de Link*, (LCP) é usado em cima de HDLC para negociar opções relacionadas com a ligação de dados.

Para
exemplo, o *Máxima receber unidade* (MRU), estabelece o tamanho máximo do datagrama que um lado do link concorda para receber.

Um passo importante na fase de configuração de um link PPP é a autorização do cliente. Embora não seja obrigatório, é realmente necessário para linhas discadas, a fim de impedir a entrada de intrusos. Normalmente, o host chamado (o servidor) pede ao cliente
autorizar-se por provar que sabe alguma chave secreta. Se o chamador não consegue produzir o segredo correto, a con-
conexão for encerrada. Com a PPP, a autorização funciona nos dois sentidos, o chamador também pode pedir ao servidor para autenti-
Cate si. Estes procedimentos de autenticação são totalmente independentes umas das outras. Existem dois protocolos para diferentes tipos de autorização, que discutiremos mais adiante neste capítulo: *Password Authentication Protocol* (PAP) e *Challenge Handshake Authentication Protocol* (CHAP).

Cada protocolo de rede que é encaminhado através de um enlace de dados (como o IP e AppleTalk) é configurado

dinamicamente
através de um correspondente *Network Control Protocol* (NCP). Para enviar datagramas IP através da ligação, os dois lados de execução
ning PPP deve primeiro negociar o endereço IP de cada um deles utiliza. O protocolo de controle utilizado para esta negociação é o *Internet Protocol Control Protocol* (IPCP).

Além de enviar datagramas IP padrão através do link, o PPP também suporta compressão de cabeçalho Van Jacobson de datagramas IP. Esta técnica reduz os cabeçalhos dos pacotes TCP para tão pouco como três bytes. Também é utilizado em CSLIP, e é mais popularmente conhecido como compressão de cabeçalho VJ. O uso de compressão pode ser nego-
ated no momento da inicialização através IPCP, também.

PPP no Linux

No Linux, a funcionalidade de PPP é dividido em duas partes: um componente do kernel que lida com os protocolos de baixo

nível

(HDLC, IPCP, IPXCP, etc) eo espaço de usuário `pppd` daemon que controla os vários protocolos de nível superior, tal como o PAP e CHAP. A versão atual do software para Linux PPP contém o daemon PPP `pppd` e um programa chamado `chat` que automatiza a marcação do sistema remoto.

O driver kernel PPP foi escrito por Michael Callahan e retrabalhadas por Paul Mackerras. `pppd` foi derivado de uma implementação PPP livre[47] para a Sun e máquinas 386BSD que foi escrito por Drew Perkins e outros, ate manido por Paul Mackerras. Ele foi portado para Linux por Al Longyear. O chat foi escrito por Karl Fox.[48]

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

45 Relevante RFCs estão listados na Bibiliography no final deste livro.

46 Na verdade, HDLC é um protocolo muito mais geral elaborado pela International Standards Organization (ISO) e é também uma componente da especificação X.25.

47 Se você tiver dúvidas gerais sobre a PPP, perguntar às pessoas na lista de discussão Linux-líquido em *vger.rutgers.edu*.

48 Karl pode ser alcançado em karl@morningstar.com.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Como SLIP, PPP é implementado por uma disciplina da linha especial. Para usar uma linha de série, como um link PPP, você primeiro estabelecer
a ligação ao longo do seu modem, como de costume, e, posteriormente, converter a linha para o modo de PPP. Neste modo, todas as in-
dados que vêm é passado para o driver PPP, que verifica os quadros de entrada HDLC de validade (cada HDLC
frame carrega um checksum de 16 bits), e desembrulha e despacha-los. Atualmente, o PPP é capaz de transportar tanto o
O protocolo IP, opcionalmente, usando a compressão de cabeçalho Van Jacobson, eo protocolo IPX.

pppd auxilia o driver do kernel, executando a inicialização ea fase de autenticação que é necessária antes de reais
tráfego de rede pode ser enviado através do link. pppd"Comportamento s podem ser afinadas com uma série de opções. Como
PPP é bastante complexo, é impossível explicar todos eles em um único capítulo. Este livro, portanto, não pode
abranger todos os aspectos pppd, Mas apenas lhe dá uma introdução. Para obter mais informações, consulte *Usando e Gestão PPP* ou o pppd páginas de manual e *README*s na pppd distribuição do código fonte, que deve lhe ajudar a resolver
a maioria das questões deste capítulo não discutir. O PPP-HOWTO também pode ser útil.

Provavelmente a maior ajuda que você vai encontrar na configuração PPP virão de outros usuários da distribuição Linux no

mesmo
buição. perguntas de configuração PPP são muito comuns, de modo a tentar sua lista de discussão ou grupo de usuários Linux do IRC
canal. Se o problema persistir mesmo após ter lido a documentação, você pode tentar o comp.protocols.ppp
newsgroup. Este é o lugar onde você pode encontrar a maioria das pessoas envolvidas no pppd de desenvolvimento.

Correndo pppd

Quando você quer se conectar à Internet através de um link PPP, você tem que configurar os recursos de rede básica,
como o dispositivo de loopback e os resolver. Ambos foram abordados no Capítulo 5, *Configurando o TCP Net / IP-trabalho*, E no capítulo 6, *Nome do serviço e configuração Resolver*. Você pode simplesmente configurar o servidor de nomes
de seu Internet Service Provider na */ Etc / resolv.conf* arquivo, mas isto significa que cada pedido é enviado DNS
através de sua conexão serial. Esta situação não é ideal, o mais próximo (em termos de rede) que está ao seu servidor de nome, o
mais rápido as pesquisas nome será. Uma solução alternativa é configurar um servidor de nomes somente de cache em um host
sua rede. Isto significa que a primeira vez que você faz uma consulta DNS para um determinado host, seu pedido será
enviadas através de sua ligação em série, mas todos os pedidos subsequentes serão respondidas diretamente pelo servidor de nome local,
e será muito mais rápido. Essa configuração é descrita no capítulo 6, em "cache-somente o nome de configuração".

Como um exemplo de introdução de como estabelecer uma conexão PPP com pppd, Suponha que você está em *vlager*

novamente.
Em primeiro lugar, discar para o servidor PPP *C3PO* e fazer login no *ppp* consideração. *C3PO* será executado o seu driver PPP. Depois de sair
o programa de comunicação que você usou para discagem, execute o seguinte comando, substituindo o nome da
dispositivo serial você utilizou para o ttyS3 mostrado aqui:

```
# pppd / dev/ttyS3 38400 crtscts defaultroute
```

Este comando inverte a linha serial *ttyS3* para a disciplina de linha PPP e negocia um link com IP *C3PO*. A trans-
fer velocidade usada na porta serial será 38.400 bps. A *crtscts* opção liga handshake de hardware na porta,
que é uma necessidade absoluta em velocidades acima de 9.600 bps.

A primeira coisa pppd se após o arranque é negociar várias características link com o terminal remoto através
LCP. Normalmente, o conjunto padrão de opções pppd tenta negociar irá funcionar, por isso não vamos entrar nesse aqui. Esperar
dizer que parte dessa negociação envolve requerente ou atribuir os endereços IP em cada extremidade da ligação.

Por enquanto, nós também assumir que a *C3PO* não requer qualquer tipo de autenticação de nós, por isso a configuração do
fase é concluída com êxito.

pppd Em seguida, negociar os parâmetros de IP com seus pares utilizando IPCP, o protocolo de controle IP. Uma vez que não
especificar qualquer endereço IP específico para pppd anteriormente, ele vai tentar usar o endereço obtido fazendo com que o resolvedor
procurar o hostname local. Ambos, então, anunciar os seus endereços para o outro.

Normalmente, não há nada de errado com esses padrões. Mesmo que sua máquina esteja em uma rede Ethernet, você pode usar o

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

mesmo
Endereço IP de Ethernet e interface PPP. No entanto, `pppd` permite que você utilize um endereço diferente,
ou mesmo de perguntar ao seu par para usar algum endereço específico. Essas opções serão discutidas posteriormente no
"Configuração de IP
Opções "seção.

Depois de passar pela fase de instalação IPCP, `pppd` vai preparar a sua camada de rede do host para usar o link PPP. É
configura a primeira interface de rede PPP como um link ponto-a-ponto, utilizando-se *ppp0* para a ligação primeira PPP que está ativa,
`ppp1` para o segundo, e assim por diante. Em seguida, ele cria uma entrada na tabela de roteamento que aponta para o acolhimento do outro lado do
link. No exemplo anterior, `pppd` fez o ponto da rota padrão da rede para *C3PO*, Porque lhe deu a *de-*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

faultroute opção.[49] TEle rota padrão simplifica o roteamento, fazendo com que qualquer datagrama IP destinado a uma não-local de acolhimento para ser enviado para *C3PO*, O que faz sentido, pois é a única maneira que pode ser alcançado. Há uma série de diferentes esquemas de roteamento `pppd` apoia, a qual será abordada em detalhe mais tarde neste capítulo.

Usando arquivos de opções

Antes `pppd` analisa seus argumentos de linha de comando, ele verifica a vários arquivos de opções padrão. Esses arquivos

podem con-
contenha quaisquer argumentos válidos de linha de comando espalhadas por um número arbitrário de linhas. Hash apresentar sinais
comentários.

O arquivo de opções do primeiro é */ Etc / ppp / options*, Que sempre é verificado quando `pppd` inicia. Usá-lo para definir

algumas
padrões globais é uma boa idéia, pois permite-lhe manter os seus usuários de fazer várias coisas que podem com-promessa de segurança. Por exemplo, para fazer `pppd` requerem algum tipo de autenticação (PAP ou CHAP) de
o ponto, adicione o *auth* opção para este ficheiro. Esta opção não pode ser substituída pelo usuário, portanto, torna-se im-vel estabelecer uma conexão PPP com qualquer sistema que não está em seus bancos de dados de autenticação. Observe, entretanto,
que algumas opções podem ser substituídos, a *contato* string é um bom exemplo.

O arquivo de outras opções, que é lido após */ Etc / ppp / options*, É *. Pprc* no diretório home do usuário. Ele permite que cada usuário especificar seu próprio conjunto de opções padrão.

Uma amostra de */ Etc / ppp / options* arquivo pode ter este aspecto:

```
# Opções para o pppd Global em execução no vlager.vbrew.com
bloqueio              # Utilização de um dispositivo de bloqueio UUCP estilo
auth                  # Exigir autenticação
UseHostName           # Usar host local para CHAP
vbrew.com domínio     # Nosso nome de domínio
```

A *bloqueio* palavra-chave faz `pppd` cumprir com o método padrão de bloqueio UUCP dispositivo. Com essa convenção, cada processo que acessa um dispositivo serial, por exemplo */ Dev/ttyS3*, Cria um arquivo de bloqueio com um nome como *LCK .. ttyS3* em
diretório de bloqueio de arquivo especial para indicar que o dispositivo está em uso. Isso é necessário para evitar sinais de outros programas,
como `minicom` ou `uucico`, Desde a abertura do dispositivo serial, enquanto ele é usado pelo PPP.

Os próximos três opções relacionadas à autenticação e, portanto, a segurança do sistema. As opções de autenticação são melhores colocados no arquivo de configuração global porque são "privilegiados" e não pode ser substituído por usuários *~ /. Pprc* arquivos de opções.

Usando o bate-papo para automatizar discagem

Uma das coisas que você pode ter impressionado como inconveniente no exemplo anterior é que você teve para estabelecer a conexão manualmente antes de poder disparar `pppd`. Diferentemente `mergulho`,`pppd` não tenha o seu próprio script linguagem de marcação do sistema remoto e login, mas depende de um programa externo ou um script shell para fazer isso. O comando a ser executado pode ser dada a `pppd` com o *contato* linha de comando opção. `pppd` redireccionado entrada padrão do comando ea saída para a linha serial.

A `pppd` pacote de software é fornecido com um programa muito simples chamado `chat`, Que é capaz de ser utilizado desta forma simples para automatizar seqüências de login. Vamos falar sobre este comando em algum detalhe.

Se a sua seqüência de login é complexa, você vai precisar de algo mais poderoso do que `chat`. Uma alternativa útil você pode considerar é `esperar`, Escrito por Don Libes. Tem uma linguagem muito poderosa baseada em Tcl, e foi concebido exatamente para este tipo de aplicação. Aqueles de vocês cujo login seqüência exige, por exemplo, desa-lenge autenticação / resposta envolvendo calculadora-como geradores de chave vai encontrar `esperar` poderoso o suficiente para
lidar com a tarefa. Uma vez que existem tantas variações possíveis sobre este tema, não vamos descrever como desenvolver um adequado esperar script neste livro. Basta dizer, você chamar seu script esperar, especificando seu nome, utilizando

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

o pppd *contato* opção. É também importante notar que quando o script está sendo executado, o padrão de entrada e saída será anexado ao modem, não para o terminal que o invocou pppd. Se você precisar de interação com o usuário, você deve gerenciá-lo através da abertura de um terminal de reposição virtual, ou arranjar outros meios.

[49] A rota de rede padrão é instalado somente se nenhum estiver presente.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A `chat` comando permite que você especifique um estilo de UUCP chat script. Basicamente, um script de bate-papo é composto por uma alternância
seqüência de seqüências que esperamos receber do sistema remoto, e as respostas que estamos a enviar. Nós chamá-los *esperar* e *enviar* cordas, respectivamente. Este é um trecho típico de um script de chat:

```
ogin: B1FF ssword: S3 | r1t <
```

Este script diz `chat` esperar para o sistema remoto para enviar o aviso de login e retornar o nome de login *B1FF*. Nós espere só para *ogin:* de modo que não importa se inicia o prompt de login com uma letra maiúscula ou minúscula l, ou se chega ilegível. A seqüência seguinte é esperar outra string que faz `chat` aguardar a solicitação de senha e enviar nossa senha resposta.

Isto é basicamente o chat scripts são tudo. Um script completo para um servidor dial-up PPP seria, naturalmente, também tem de incluir os comandos de modem apropriado. Suponha que o modem entende o comando Hayes definido, eo número do servidor de telefone é 318714. O completo `chat` invocação para estabelecer uma conexão com *C3PO* seria então:

```
$ chat-v''ATZ OK''CONNECT ATDT318714 ogin: palavra PPP: Gagarin
```

Por definição, a primeira seqüência de caracteres deve ser uma seqüência de esperar, mas como o modem não vou dizer nada antes de ter
chutou, fazemos `chat` ignorar os primeiros esperam especificando uma seqüência vazia. Em seguida, enviar *ATZ*, Com o reset demanda por modems Hayes-compatible, e esperar por sua resposta (*OK*). A próxima seqüência envia a `dial` comando juntamente com o número de telefone `chat`, E espera que a *CONNECT* mensagem em resposta. Isso é seguido por um string vazia novamente, porque nós não queremos enviar alguma coisa agora, mas sim aguardar o aviso de login. A re-mainder do script de chat funciona exatamente como descrito anteriormente. Essa descrição provavelmente parece um pouco confuso, mas vamos ver em um momento que há uma maneira de fazer scripts chat muito fácil de entender.

A *-V* opção faz com que `chat` registrar todas as atividades para o `syslog` daemon *LOCAL2* facilidade.[50]

Especificando o chat script na linha de comando tem um certo risco, pois os usuários podem visualizar o comando de um processo
consonância com o `ps` comando. Você pode evitar esse risco, colocando o script de chat em um arquivo como *dial-C3PO*. Você faz
`chat` li o roteiro a partir do arquivo em vez da linha de comando, dando-lhe o *-F* opção, seguido pelo arquivo nome. Esta ação tem a vantagem de tornar o nosso chat esperar seqüências mais fácil de entender. Para converter nosso exemplo, nossa *dial-C3PO* arquivo ficaria assim:

```
''      ATZ
OK      ATDT318714
CONNECT''
ogin:   ppp
palavra:    Gagarin
```

Quando usamos um arquivo de script de bate-papo, desta forma, a seqüência que espera receber é a da esquerda e da resposta que vai
enviar é à direita. Eles são muito mais fáceis de ler e compreender quando se apresenta desta forma.

O completo `pppd` encantamento olharia agora como esta:

```
# pppd connect "chat-f dial C3PO" / dev/ttyS3 38.400 destacam-\
        crtscts modem defaultroute
```

Além da *contato* opção que especifica o script dial-up, nós adicionamos mais duas opções para a linha de comando: *Destacam-*, Que diz `pppd` não destacar a partir do console e tornar-se um processo de fundo, e os *modem* palavra-chave, o que torna executar ações modem específico sobre o dispositivo serial, como desligar a linha antes e após a chamada. Se você não usar esta palavra-chave `pppd` não vai acompanhar a linha DCD porto e, portanto, Não foi possível detectar se o final remoto desliga inesperadamente.

Os exemplos que temos mostrado é bastante simples; `chat` permite muito mais complexos scripts. Por exemplo, pode especificar strings em que abortar a conversar com um erro. seqüências de abortar típicos são mensagens como *BUSY* ou *NO CARRIER* que o seu modem normalmente gera quando o número chamado está ocupado ou não atende. Para fazer `chat` reconhecer imediatamente estas mensagens ao invés de atingir o tempo limite, você pode especificá-los no início do script usando o *ABORT* palavra-chave:

```
$ chat-v ABORT BUSY ABORT 'NO CARRIER''ATZ OK ...
```

Da mesma forma, você pode alterar o valor de tempo limite para as partes dos scripts de chat, inserindo *TIMEOUT* opções.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

50 Se você editar *syslog.conf* para redirecionar essas mensagens de log para um arquivo, verifique se este arquivo não é legível, como `chat` também registra todo o chat
script por padrão - incluindo senhas.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Às vezes, você também precisa ter a execução condicional de partes do script de bate-papo: quando você não receber o login remoto final do alerta, você pode querer enviar uma pausa ou um retorno de carro. Você pode conseguir este ap- na pendência de um índice para uma seqüência de esperar. O índice é composto por uma seqüência de seqüências de enviar e esperar, assim como
o script global em si, que são separadas por hífens. O índice é executado sempre que o string esperado
é anexado não for recebido a tempo. No exemplo acima, poderíamos modificar o chat script como segue:

```
ogin:-BREAK-ogin: ssword PPP: Gagarin
```

Quando `chat` não vê o sistema remoto enviar o prompt de login, o índice é executado através do envio de um BREAK, e depois esperar para o prompt de login novamente. Se o prompt aparece agora, o script continua normalmente; Caso contrário, ele irá terminar com um erro.

Opções de configuração de IP

IPCP é usado para negociar uma série de parâmetros IP no momento da configuração da ligação. Normalmente, cada peer envia

uma IPCP
Configuração do pacote pedido, indicando quais os valores que quer mudar a partir dos padrões e do novo valor. Após a recepção, na extremidade remota inspeciona cada opção de cada vez e nem admite ou rejeita-la.

`pppd` dá-lhe um grande controle sobre as opções IPCP ele vai tentar negociar. Você pode ajustá-la através de vários opções de linha de comando que vamos discutir nesta seção.

A escolha de endereços IP

Todas as interfaces IP exigem endereços IP atribuídos a eles, um dispositivo de PPP sempre tem um endereço IP. O conjunto de

PPP
protocolos fornece um mecanismo que permite a atribuição automática de endereços IP para interfaces PPP. É possível para o programa de PPP em uma extremidade de um link ponto-a-ponto para atribuir um endereço IP para o final remoto para utilizar,
ou cada um pode usar o seu próprio.

Alguns servidores PPP que lidar com um monte de sites de clientes atribuir endereços dinamicamente, os endereços são

atribuídos aos sis-
tems somente quando chamada dentro e são recuperados depois de terem registrado novamente. Isso permite que o número de anúncios IP
vestidos devem ser limitadas ao número de linhas discadas. Enquanto a prescrição é conveniente para os gestores das PPP servidor dial-up, muitas vezes é menos conveniente para os usuários que estão de marcação dentro Discutimos a forma como hostnames
são mapeados para endereços IP através do uso de um banco de dados no Capítulo 6. Para que as pessoas se conectar ao seu host, eles
deve saber seu endereço IP ou o nome do host associado a ele. Se você é um usuário de um serviço de PPP que lhe atribui um endereço IP dinamicamente, esse conhecimento é difícil, sem fornecer alguns meios de permitir que os dados DNS base para ser atualizado depois que você é atribuído um endereço IP. Esses sistemas existem, mas não vamos cobri-los em detalhe
aqui, em vez disso, vamos olhar para a abordagem mais preferível, que envolve você poder usar o mesmo IP endereço de cada vez que você estabeleça sua conexão de rede.[51]

No exemplo anterior, tínhamos `pppd` dial-up *C3PO* e estabelecer uma ligação IP. Não há disposições foram tomadas para

escolher
~~um determinado endereço IP em cad~~a extremidade da ligação. Em vez disso, nós vamos `pppd` ter sua ação padrão. É uma tentativa de re-
resolver o hostname local, *vlager* No nosso exemplo, para um endereço IP, que utiliza para o local final, ao deixar a máquina remota, *C3PO*, Fornecer seu próprio. PPP apóia várias alternativas para este arranjo.

Para pedir a determinados endereços, você geralmente fornecem `pppd` com a seguinte opção:

LOCAL_ADDR:*REMOTE_ADDR*

LOCAL_ADDR e *REMOTE_ADDR* pode ser especificado em notação decimal com pontos ou como hostnames.[52] Esta opção faz `pppd` tentativa de usar o primeiro endereço fornecido como seu próprio endereço IP, eo segundo como o de pares. Se o

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

pares rejeita qualquer um dos endereços durante a negociação IPCP, nenhuma ligação IP será estabelecida.[53]

Se você estiver discando para um servidor e esperar que atribuir-lhe um endereço IP, você deve garantir que pppd não tentativa de negociar um por si. Para fazer isso, use o *noipdefault* opção e sair do *LOCAL_ADDR* em branco. A

51 Mais informações sobre dois mecanismos de atribuição dinâmica de acolhimento pode ser encontrada em http://www.dynip.com/ e http://www.justlinux.com/dynamic_dns.html.

52 Usando nomes de host nesta opção tem consequências para a autenticação de CHAP. Por favor, consulte a seção "Autenticação com PPP" seção mais adiante neste capítulo.

53 A *IPCP-accept-local* e *IPCP-accept-remote* opções de instruir seu pppd para aceitar o IP local e remoto endereços estão sendo oferecidos por o PPP remoto, mesmo que você tenha fornecido algum em sua configuração. Se essas opções não estão configurados, o pppd rejeitará qualquer na- tentar negociar os endereços IP usados.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

noipdefault opção vai parar `pppd` ao tentar usar o endereço IP associado ao nome do host como o local endereço.

Se você quer definir apenas o endereço do local, mas aceita qualquer endereço o par utiliza, simplesmente deixar de fora o

REMOTE_ADDR
peça. Para fazer *vlager* usar o endereço IP *130.83.4.27* em vez de seus próprios, dar-lhe *130.83.4.27:* sobre o comando linha. Da mesma forma, para definir o endereço remoto apenas, deixar o *LOCAL_ADDR* campo em branco. Por padrão, `pppd` Em seguida, use
o endereço associado ao seu nome.

Roteamento Através de um link PPP

Depois de configurar a interface de rede, `pppd` normalmente irá criar uma rota de anfitrião aos seus pares somente. Se o host

remoto está
em uma LAN, você certamente quer ser capaz de se conectar a hosts "atrás" de seus pares, bem como, nesse caso, uma rede rota deve ser configurada.

Nós já vimos que `pppd` pode ser solicitado para definir a rota padrão usando o *defaultroute* opção. Esta opção é muito útil se o servidor PPP discado até funciona como seu gateway de Internet.

O caso inverso, em que o sistema age como um gateway para um único hospedeiro, é relativamente fácil de realizar. Por exemplo, levar algum funcionário da Cervejaria Virtual, cuja casa de máquina é chamada *oneshot*. Vamos também assumir que temos configurado *vlager* como um servidor PPP de discagem. Se tiver configurado *vlager* para atribuir dinamicamente um
Endereço IP que pertence à sub-rede da cervejaria, então podemos usar o *proxyarp* opção com `pppd`, Que será instalar uma entrada ARP proxy para *oneshot*. Isso faz com que *oneshot* acessível a todos os hosts na Cervejaria e da adega.

No entanto, as coisas nem sempre são tão simples assim. Ligando duas redes locais geralmente requer a adição de um

determinado
via rede, pois essas redes podem ter suas rotas padrão próprio. Além disso, ter dois pares usar o PPP ligação como a rota padrão geraria um loop, por meio do qual os pacotes para destinos desconhecidos que ping-pong entre os pares, até o seu tempo para viver expirado.

Suponha que a cervejaria virtual abre uma filial em outra cidade. A subsidiária da funciona uma rede Ethernet de seu próprio

utilizando o
Número de rede IP *172.16.3.0*, Que é sub-3 da rede de classe B da cervejaria. A filial quer se conectar à rede da cervejaria via PPP para atualizar bases de dados do cliente. Mais uma vez, *vlager* age como um gateway para
a rede de cervejarias e apoiará o link PPP; seus pares no novo ramo é chamado *vbourbon* e tem um IP endereço do *172.16.3.1*. Esta rede é ilustrada na Figura 24,2 no Apêndice A, *Rede Exemplo: A Virtual Cervejaria*.

Quando *vbourbon* conecta-se a *vlager*, Faz o ponto da rota padrão para *vlager* como de costume. Em *vlager*No entanto, nós terá apenas a rota ponto-a-ponto para *vbourbon* e terá que especialmente configurar uma rota de rede para a sub-líquida que usa três *vbourbon* como seu gateway. Nós poderíamos fazer isso manualmente usando o `rota` comando à mão após o ligação PPP é estabelecida, mas isso não é uma solução muito prática. Felizmente, nós podemos configurar a auto-route automaticamente usando um recurso de `pppd` que nós não discutimos ainda - a `ip-up` comando. Este comando é um shell script ou programa localizado na */ Etc / ppp* que é executado pelo `pppd` após a interface PPP foi configurado. Quando presente, ela é invocada com os seguintes parâmetros:

`ip-up` *iface dispositivo REMOTE_ADDR LOCAL_ADDR velocidade*

A seguinte tabela resume o significado de cada um dos argumentos (na primeira coluna, vamos mostrar o número usado pelo script para se referir a cada argumento):

Argumento	Nome	Finalidade
$ 1	$ 2	

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

$ 3	*iface*	A interface de rede usada, por exemplo, `ppp0`
	dispositivo	O caminho do arquivo de dispositivo serial utilizada (*/ Dev / tty*, Se stdin / stdout são usados)
	velocidade	A velocidade do dispositivo serial em bits por segundo
$ 4	*LOCAL_ADDR*	O endereço IP do terminal remoto do link com pontos

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Argumento	Nome	Finalidade
$ 5	*REMOTE_ADDR*	O endereço IP do terminal remoto do link em notação decimal com pontos

No nosso caso, o `ip-up` script pode conter o seguinte fragmento de código:[54]

```
#! / Bin / sh
caso $ 5 em
172.16.3.1)            # Isto é vbourbon
        route add-net gw 172.16.3.0 172.16.3.1;;
...
esac
exit 0
```

Da mesma forma, `/ Etc / ppp / ip-down` pode ser usado para desfazer qualquer ação de `ip-up` depois do link PPP foi tomada
para baixo novamente. Assim, em nosso `/ Etc / ppp / ip-down` script teríamos uma `rota` comando que removeu o percurso que criamos no `/ Etc / ppp / ip-up` script.

No entanto, o esquema de roteamento ainda não está completa. Temos um conjunto de entradas de tabela de roteamento em ambos os anfitriões PPP, mas também
agora, nenhum dos hosts em cada rede sabe alguma coisa sobre a ligação PPP. Este não é um grande problema se todos os hosts na subsidiária tem sua rota padrão apontando para *vbourbon*, E todos Cervejaria rota hosts *vlager* por padrão.
Se este não for o caso, sua única opção é geralmente a usar um daemon de roteamento como `gated`. Depois de criar a rede-rota de trabalho em *vlager*, As transmissões daemon de roteamento a nova rota para todos os hosts da sub-inscritos.

Opções de Controle Link

Nós já encontramos o Link Control Protocol (LCP), que é usado para negociar características link e teste o link.

As duas opções mais importantes negociados pela LCP são os *Asynchronous Mapa de Caracteres de controle* e *Máxima receber unidade*. Há uma série de outras opções de configuração LCP, mas eles são muito especializadas para discutir aqui.

O controle assíncrono Mapa de Caracteres, coloquialmente chamado de *Mapa async*, É usado em ligações assíncronas, tais como linhas telefônicas, para identificar caracteres de controle que deve ser escapado (substituído por um de dois caracteres específicos
seqüência) para evitar que sejam interpretados por equipamentos utilizados para estabelecer o link. Por exemplo, você pode querer
evitar os caracteres XON e XOFF usado para aperto de software, porque um modem configurado incorretamente pode engasgar após recepção de um XOFF. Outros candidatos incluem-l Ctrl (o `telnet` caractere de escape). PPP permite que você escapam a qualquer um dos caracteres com códigos ASCII de 0 a 31, especificando-os no mapa async.

O mapa async é um bitmap de 32 bits de largura, expresso em hexadecimal. O bit menos significativo corresponde à ASCII caractere NULL, eo bit mais significativo corresponde ao decimal ASCII 31. Estes 32 ASCII caractros são os caracteres de controle. Se um bit é definido no mapa de bits, sinaliza que o personagem correspondente deverá ser escaparam antes que ele seja transmitido através do link.

Para dizer ao seu par que não tem de escapar a todos os caracteres de controle, mas apenas alguns deles, você pode especificar um
mapa para async `pppd` usando o *asyncmap* opção. Por exemplo, se só `S ^` e `^ Q` (ASCII 17 e 19, vulgarmente utilizados para XON e XOFF) deve ser precedido, use a opção a seguir:

```
asyncmap 0x000a0000
```

A conversão é simples, desde que você pode converter binário para hexadecimal. Lay out 32 bits na frente de você. O direito do corresponde a pouco mais de ASCII 00 (NULL), eo bit mais à esquerda corresponde a ASCII decimal 32. Definir os bits correspondentes aos caracteres que você deseja fugiu para um lado, ea todos os outros a zero. Para converter isso para o hexa-número decimal `pppd` espera, basta tomar cada conjunto de 4 bits e convertê-los em hexadecimal. Você deve acabar com oito dígitos hexadecimais. Agregá-los todos juntos e preprend "0x" para significar que é um número hexadecimal, e

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

você está feito.

54 Se quiséssemos ter rotas para outros sites criados quando discar, nós adicione declarações eventualmente, para cobrir aqueles em que a `. . .` aparece no exemplo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Inicialmente, o mapa async é definido como `0xffffffff` - Isto é, todos os caracteres de controle não serão escapados. Esta é uma forma segura
padrão, mas normalmente é muito mais do que você precisa. Cada personagem que aparece no mapa async resultados em dois
caracteres a ser transmitido através do link, para escapar está no custo de utilização do link e um aumento redução do desempenho correspondente.

Na maioria dos casos, um mapa de async `0x0` funciona bem. Não há escapatória é executada.

O máximo receber Unit (MRU), os sinais para o ponto o tamanho máximo de quadros HDLC queremos receber. Embora isso possa lembrá-lo do valor unitário de transferência máxima (MTU), estes dois têm pouco em comum. A MTU é um parâmetro do dispositivo de rede do kernel e descreve o tamanho máximo a interface é capazes de transmitir. O MRU é mais um conselho para o fim remoto para não gerar quadros maior do que o MRU; a interface deve, no entanto, ser capaz de receber imagens de até 1.500 bytes.

A escolha de um MRU, não é tanto uma questão do que a ligação é capaz de transferir, mas do que dá-lhe a melhor taxa de transferência. Se você pretende executar aplicativos interativos sobre o link, a configuração da MRU para
valores tão baixos como 296 é uma boa idéia, para que um pacote ocasionais de maior dimensão (digamos, de uma sessão FTP) não faz
o cursor "pular". Para dizer `pppd` para solicitar um MRU de 296, você dá a ele a opção `mru 296`. MRUs Pequeno, No entanto, só fazem sentido se você tiver a compressão de cabeçalho VJ (ele é ativado por padrão), porque senão você desperdiçar uma grande quantidade de sua largura de banda apenas de carregar o cabeçalho IP para cada datagrama.

`pppd` também compreende um par de opções LCP que configuram o comportamento global do processo de negociação, tais como o número máximo de pedidos de configuração que podem ser trocadas antes da ligação é encerrada. A menos que você saiba exatamente o que você está fazendo, você deve deixar estas opções sozinho.

Finalmente, há duas opções que se aplicam a LCP mensagens de eco. PPP define duas mensagens, *Echo Request* e *Echo Resposta*.`pppd` usa esse recurso para verificar se um link ainda está operando. Você pode habilitar isso usando o *LCP-echo-interval* opção juntamente com um tempo em segundos. Se não houver quadros são recebidos a partir do host remoto dentro desta
intervalo, `pppd` gera uma solicitação de eco e espera que os colegas para retornar uma resposta de eco. Se o ponto não produzir uma resposta, a ligação é encerrada após um certo número de pedidos são enviados. Este número pode ser definido usando o *lcp-echo-falha* opção. Por padrão, esse recurso será desativado.

Considerações de Segurança Geral

A errada daemon PPP pode ser uma violação de segurança devastador. Ela pode ser tão ruim como deixar qualquer um plug seu máquina em sua rede Ethernet (e que pode ser muito ruim). Nesta seção, discutimos algumas medidas que devem fazer a sua configuração PPP segura.

Observação: privilégios de root é necessária para configurar o dispositivo de rede e tabela de roteamento. Você normalmente irá resolver este
pela execução `pppd` setuid *root*. No entanto, `pppd` permite aos usuários configurar várias opções de segurança relevantes.

Para se proteger contra qualquer ataque de um usuário pode lançar através da manipulação `pppd` opções, você deve definir um par de
valores padrão no mercado global */ Etc / ppp / options* arquivo, como as mostradas no arquivo de exemplo em "Usando arquivos de opções",
anteriormente neste capítulo. Alguns deles, como as opções de autenticação, não pode ser substituída pelo usuário, e assim proporcionar uma protecção razoável contra manipulações. Uma importante opção para proteger o *contato* opção. Se pretende permitir que os usuários não-raiz para invocar `pppd` para se conectar à Internet, você deve sempre adicionar o `connect` e `noauth` opções para o arquivo de opções globais */ Etc / ppp / options*. Se você não fizer isso, os usuários serão capazes de
executar comandos arbitrários com `root` privilégios, especificando o comando como seu *contato* comando sobre o `pppd` linha ou em seu arquivo de opções pessoais.

Outra boa idéia é restringir quais usuários podem executar `pppd` criando um grupo de */ Etc / group* e adicionando somente os usuários que você deseja ter a capacidade de executar o daemon PPP. Você deve então mudar de grupo propriedade da `pppd` daemon a esse grupo e remover o mundo privilégios de execução. Para fazer isso, supondo

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

você ligou o seu grupo *dialout*, Você poderia utilizar algo como:

```
#  chown root / usr / sbin / pppd
#  dialout chgrp / usr / sbin / pppd
#  chmod 4750 / usr / sbin / pppd
```

Claro, você tem que se proteger dos sistemas de falar com PPP, também. Para afastar os hosts colocam como outra pessoa, você deve sempre exigir algum tipo de autenticação do seu par. Além disso, você deve

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

não permitir que hosts externos para usar qualquer endereço IP que escolhem, mas restringi-las ao máximo de alguns. Os seguintes sec-
ção irá lidar com esses tópicos em detalhes.

Autenticação com PPP

Com a PPP, cada sistema pode precisar de seus pares para se autenticar usando um dos dois protocolos de autenticação: o *Password Authentication Protocol* (PAP), e os *Challenge Handshake Authentication Protocol* (CHAP).
Quando uma conexão é estabelecida, em cada extremidade pode pedir a outra para autenticar a si mesmo, independentemente de se tratar de
o chamador ou o receptor. Na descrição que se segue, vamos falar vagamente de "cliente" e "servidor" quando queremos para distinguir entre o sistema de envio de solicitações de autenticação eo sistema responder a elas. A PPP
daemon pode pedir a seus pares para a autenticação através do envio de mais um pedido de configuração LCP identificar os desejado protocolo de autenticação.

PAP CHAP Versus

PAP, que é oferecido por muitos provedores de Internet, funciona basicamente da mesma forma que o login normal procedimento. O cliente autentica-se através do envio de um username e uma senha (opcionalmente criptografados) para o servidor, que o servidor se compara ao seu banco de segredos.[55] Esta técnica é vulnerável a intrusos, que pode tentar obter a senha através da escuta em série na linha, e repetidos ataques de tentativa e erro.

CHAP não tem essas deficiências. Com CHAP, o servidor envia um gerado aleatoriamente "desafio" string para o cliente, juntamente com seu nome. O cliente usa o nome da máquina para procurar o segredo disso, combina-
com o desafio, e criptografa a string usando uma função hash unidirecional. O resultado é devolvido ao servidor junto com o hostname do cliente. O servidor agora executa o mesmo cálculo, e reconhece o cliente se que chegue ao mesmo resultado.

CHAP também não exige que o cliente autenticar-se apenas no momento da inicialização, mas envia desafios em regular intervalos para se certificar de que o cliente não tenha sido substituído por um intruso, por exemplo, linhas telefónicas de comutação, ou
devido a um erro de configuração do modem que faz com que o daemon PPP não perceber que o telefonema original tem retirou-se e alguém tem marcado dentro

pppd mantém as chaves secretas para o PAP e CHAP em dois arquivos separados denominados */ Etc / ppp / pap-secrets* e */ Etc / ppp / chap-secrets*. Ao entrar em um host remoto em um ou outro arquivo, você tem um controle fino sobre se PAP ou CHAP é usado para autenticar-se com seu colega, e vice-versa.

Por padrão, pppd não necessitam de autenticação do host remoto, mas ele vai acordar para autenticar-se quando solicitado pelo host remoto. Desde CHAP é muito mais forte do PAP, pppd tenta usar o antigo sempre possível. Se o ponto de não apoiá-lo, ou se pppd não consegue encontrar um segredo de CHAP para o sistema de controle remoto em sua *chap-*
segredos arquivo, ele reverte para o PAP. Se ele não tem um segredo PAP para seus pares, quer, recusa-se a autenticar-alto juntos. Como conseqüência, a ligação é encerrada.

Você pode modificar este comportamento de várias maneiras. Quando dada a *auth* palavra-chave, pppd exige que os pares de

autên-
ticate si. pppd concorda em usar o CHAP ou PAP, enquanto ele tem um segredo para os colegas na sua CHAP ou PAP banco de dados. Há outras opções para transformar um protocolo de autenticação especial ligado ou desligado, mas não vou descrevê-los
aqui.

Se todos os sistemas de falar com com o PPP de acordo para autenticar-se com você, você deve colocar o *auth* opção global */ Etc / ppp / options* arquivo e definir senhas para cada sistema no *chap-secrets* arquivo. Se um sistema não apoio CHAP, adicione uma entrada para que o *pap-secrets* arquivo. Dessa forma, você pode ter certeza de sistemas não-autenticadas
MET se conecta ao seu host.

As duas próximas seções discutem os dois segredos arquivos PPP, *pap-secrets* e *chap-secrets*. Eles estão localizados na */ Etc / ppp* e conter trigêmeos de clientes, servidores e senhas, opcionalmente seguido por uma lista de endereços IP. A interpretação do cliente e os campos de servidor é diferente para CHAP e PAP, e também depende de nós autenticar-se com os pares, ou se nós exigimos que o servidor para autenticar-se conosco.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

55 "Secret" é apenas o nome PPP para senhas. segredos PPP não têm a mesma limitação do comprimento como senhas de login do Linux.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Os segredos CHAP Arquivo

Quando se tem de se autenticar com um servidor usando CHAP, pppd Pesquisas da *chap-secrets* arquivo para uma entrada com o campo do cliente igual ao nome do servidor local, e no campo servidor igual ao host remoto enviado no CHAP desafio. Ao exigir que o ponto para se autenticar, os papéis são simplesmente invertida: pppd então olha para uma entrada com o campo do cliente igual ao nome do host remoto (enviada em resposta do cliente CHAP), e os campo do servidor igual ao nome do servidor local.

O seguinte é uma amostra *chap-secrets* arquivo para *vlager*:[56]

```
# Segredos CHAP para vlager.vbrew.com
#
# Cliente        servidor         segredo              addrs
#------------------------------------------------ ------------------
vlager.vbrew.com  c3po.lucas.com   "Use a fonte de Lucas" vlager.vbrew.com
c3po.lucas.com    vlager.vbrew.com "arttoo! arttoo!"     c3po.lucas.com
*                 vlager.vbrew.com "TuXdrinksVicBitter"  pub.vbrew.com
```

Quando *vlager* estabelece uma conexão PPP com *C3PO*,*C3PO* pergunta *vlager* para autenticar-se através do envio de um sujeito desafio. pppd em *vlager* em seguida, verifica *chap-secrets* para uma entrada com o campo do cliente igual a *vlager.vbrew.com* e no campo servidor de igual *c3po.lucas.com*, E encontra a primeira linha mostrada no exemplo.[57] É produz então o CHAP resposta da seqüência de desafio e que o segredo (`O uso Lucas Fonte`), E envia-lo para *C3PO*.

pppd Constitui um desafio CHAP para *C3PO* contendo uma seqüência de desafio único e seu totalmente qualificado hostname, *vlager.vbrew.com*.*C3PO* constrói uma resposta CHAP na forma como discutimos, e retorna ao *vlager*.pppd Em seguida, extrai o nome do host do cliente (*c3po.vbrew.com*) A partir da resposta e busca a *chap-segredos* arquivo para uma linha que corresponda *C3PO* como um cliente e *vlager* como o servidor. A segunda linha faz isso, então pppd
Combina o desafio CHAP eo segredo `arttoo! arttoo!`, Criptografa-los, e compara o resultado com *C3PO*'S resposta CHAP.

O quarto campo opcional lista os endereços IP que são aceitáveis para o cliente chamado no primeiro campo. O ad-vestidos pode ser dado com pontos ou como nomes que são procurados com o resolvedor. Por exemplo, se *C3PO* pede para usar um endereço IP durante a negociação IPCP que não está nesta lista, o pedido é rejeitado, e IPCP é fechado. No arquivo de exemplo mostrado acima, *C3PO* é, portanto, limitado a usar seu próprio endereço IP. Se o endereço campo está vazio, os endereços são permitidos; um valor "`-`"Impede o uso de IP com que o cliente por completo.

A terceira linha da amostra *chap-secrets* arquivo permite a qualquer host para estabelecer uma ligação com o PPP *vlager* porque

um cliente
ou o campo do servidor de `*` é um wildcard que qualquer hostname. As únicas exigências são que o host de conexão deve saber o segredo e que ele deve usar o endereço IP associado *pub.vbrew.com*. As entradas com curinga hostnames podem aparecer em qualquer parte do arquivo de segredos, uma vez que pppd usará sempre o melhor jogo que pode encontrar para o
servidor / cliente par.

pppd pode necessitar de alguma ajuda formando hostnames. Como explicado anteriormente, o nome do host remoto é sempre

fornecida pelo
o ponto no desafio CHAP ou pacote de resposta. O nome de host local é obtido chamando o *GetHost-nome (2)* função por padrão. Se você tiver definido o nome do sistema para o seu host não qualificados, você também tem que fornecer pppd com o nome de domínio usando o *domínio* opção:

```
# pppd ... vbrew.com domínio
```

Esta disposição acrescenta o nome da cervejaria é de domínio *vlager* para todas as actividades relacionadas com a autenticação.

Outras op-
ções que modificam pppd"Ideia s do nome do host local são *UseHostName* e *nome*. Quando você dá o IP local endereço na linha de comando usando *local*:*remoto* e *local* como um nome em vez de um quad pontilhada, pppd usa este como o nome da máquina local.

Os Segredos PAP Arquivo

O PAP arquivo segredos é muito semelhante ao CHAP é. Os dois primeiros campos sempre conter um nome de usuário e um

servidor

PDF Creator PDF4Free v2.0 http://www.pdf4free.com

nome, o terceiro guarda o segredo PAP. Quando o host remoto envia suas informações de autenticação, pppd usa o entrada que tem um campo igual ao servidor de host local e um campo de usuário igual ao nome enviado na re-

56 As aspas não são parte do segredo, pois eles servem apenas para proteger os espaços em branco dentro dele.
57 Esta máquina é retirado do desafio CHAP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

busca. Quando for necessário para que possamos enviar nossas credenciais para os pares, `pppd` usa o segredo que tem um campo de usuário
igual ao nome do usuário local e no campo servidor igual ao host remoto.

Uma amostra de PAP segredos arquivo pode ter este aspecto:

```
# / Etc / ppp / pap-secrets
#
# Usuário        servidor        segredo         addrs
vlager-pap       C3PO            cresspahl       vlager.vbrew.com
C3PO             vlager          DonaldGNUth     c3po.lucas.com
```

A primeira linha é usado para autenticar-se quando se fala de *C3PO*. A segunda linha descreve como um usuário chamado *C3PO* tem de autenticar-se conosco.

O nome *vlager-pap* na primeira coluna é o nome que enviamos para *C3PO*. Por padrão, `pppd` escolhe o local
nome do host como o nome, mas você também pode especificar um nome diferente, dando a *usuário* opção de seguir por essa nome.

Ao escolher uma entrada da *pap-secrets* arquivo para identificar-nos com um host remoto, `pppd` deve saber a distância
nome do anfitrião. Como ele não tem como descobrir isso, você deve especificá-lo na linha de comando usando o *remotename* palavra-chave seguida pelo nome da máquina do peer. Para usar a entrada acima para autenticação com *C3PO*, Por exemplo, deve adicionar a seguinte opção `pppd`'S de linha de comando:

```
# pppd ... remotename C3PO usuário vlager pap-
```

No quarto campo do arquivo segredos PAP (e todos os campos a seguir), você pode especificar quais endereços IP são allowed para um host em particular, assim como no arquivo segredos CHAP. O ponto será permitida a solicitação somente endereços
da lista. No arquivo de exemplo, a entrada que *C3PO* vai usar quando ele disca - a linha onde *C3PO* é o cliente -
permite que ele use seu endereço IP real e nenhum outro.

Note-se que a PAP é um método de autenticação mais fraca, você deve usar CHAP vez, sempre que possível. Nós
não será, portanto, abranger PAP em maiores detalhes aqui, se você estiver interessado em usá-lo, você vai encontrar mais FEAPAP
turas no *pppd (8)* manual de página.

Depuração da sua configuração de PPP

Por padrão, `pppd` registra todas as advertências e mensagens de erro `syslog`'S *daemon* facilidade. Você tem que adicionar uma entrada
para *syslog.conf* que redireciona as mensagens para um arquivo ou mesmo o console, caso contrário, `syslog` simplesmente descarta
elas. A entrada a seguir envia todas as mensagens para */ Var / log / ppp-log*:

```
daemon .*                / Var / log / ppp-log
```

Se a sua conexão PPP não funcionar imediatamente, você deve olhar neste arquivo de log. Se as mensagens de log não ajuda, você
também pode ativar a saída de depuração extra usando o *depurar* opção. Este resultado faz com que `pppd` log o conteúdo de todos
pacotes de controle enviados ou recebidos para `syslog`. Todas as mensagens depois ir para o *daemon* facilidade.

Finalmente, a forma mais drástica para verificar um problema é para ativar a depuração no nível do kernel, invocando `pppd` com o
kdebug opção. Ele é seguido por um argumento numérico que é a soma dos seguintes valores: 1 para depuração geral mensagens, 2 para imprimir o conteúdo de todos os quadros de entrada HDLC, e 4 para fazer o driver de impressão todas as saída
quadros HDLC. Para capturar as mensagens de depuração do kernel, você deve executar um `syslogd` daemon que lê o */ Proc / kmsg* arquivo, ou o `klogd` daemon. Qualquer um deles dirige a depuração do kernel para o `syslog` *kernel* facilidade.

Mais Configurações Avançadas PPP

Ao configurar PPP para discar para uma rede como a Internet é a aplicação mais comum, há aqueles
ator você que têm requisitos mais avançados. Nesta seção vamos falar sobre alguns dos mais recentes con-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

figurações possíveis com PPP no Linux.

PPP Server

Duração `pppd` como um servidor é apenas uma questão de configurar um dispositivo tty serial para invocar `pppd` com as devidas
opções quando uma chamada de dados de entrada foi recebida. Uma maneira de fazer isso é criar uma conta especial, digamos *ppp*,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

e dar-lhe um script ou programa como um shell de login que chama `pppd` com estas opções. Alternativamente, se você pretende para suportar autenticação PAP ou CHAP, você pode usar o `mgetty` programa de apoio ao seu modem e explorar seu "/ AutoPPP / recurso".

Para construir um servidor usando o método de login, você adicionar uma linha semelhante à seguinte ao seu */ Etc / passwd* arquivo:[58]

```
PPP: x: 500:200: Público Conta do PPP: / tmp: / etc / ppp / ppplogin
```

Se seu sistema suporta senhas de sombra, você também precisará adicionar uma entrada para o */ Etc / shadow* arquivo:

```
PPP:!: 10913:0:99999:7:::
```

Naturalmente, o UID e GID que você usa depende do usuário que deseja possuir a conexão, e como você criou. Você também tem que definir a senha para a conta mencionada usando o `passwd` comando.

A `ppplogin` script pode ter esta aparência:

```
#! / Bin / sh
# Ppplogin - script de fogo até o pppd no login
mesg n
stty-echo
exec pppd-desanexar silenciosa crtscts modem
```

A `mesg` comando desativa outros usuários da escrita para a tty usando, por exemplo, o `escrever` comando. A `stty` comando desliga caráter ecoando. Este comando é necessário, caso contrário, tudo o que o peer envia seria ecoada de volta para ela. O mais importante `pppd` opção dada é *Destacam-* porque impede `pppd` desprendam do controle tty. Se não especificar esta opção, ele iria para o fundo, fazendo a saída shell script. Por sua vez, faria com que o cabo serial para desligar a conexão e para ser descartado. A `silenciosa` opção faz com que `pppd` esperar até que ele recebe um pacote do sistema de chamada antes de começar a enviar. Esta opção evita transmitir timeouts ocorra quando o sistema de chamada é lento na demissão de seu cliente PPP. A *modem* opção faz com que `pppd` movimentação das linhas de modem o controle da porta serial. Você deve sempre transformar este opção pelo uso `pppd` com um modem. A *crtscts* opção liga handshake de hardware.

Além dessas opções, você pode querer forçar algum tipo de autenticação, por exemplo, especificando *auth* em `pppd`'S de linha de comando ou no arquivo de opções globais. A página do manual também aborda as opções mais específicas para transformando os protocolos de autenticação individual ligado e desligado.

Se você deseja usar `mgetty`, Tudo que você precisa fazer é configurar `mgetty` para suportar o dispositivo serial seu modem está conectada (consulte "Configurando o Daemon mgetty" para mais detalhes), configure `pppd` para o PAP ou CHAP authentication com opções adequadas no seu *opções* arquivo e, finalmente, adicionar uma seção similar à seguinte ao seu */ Etc / mgetty / login.config* arquivo:

```
# Configurar o mgetty para detectar automaticamente as chamadas PPP e invocar
# O daemon pppd para lidar com a conexão.
#
/ AutoPPP / -   ppp   / Usr / sbin / pppd chap-auth + login pap
```

O primeiro campo é uma parte especial da magia usada para detectar que uma chamada é uma PPP. Você não deve mudar o caso da cadeia, que é sensível a maiúsculas. A terceira coluna é o nome que aparece na `que` anúncios quando alguém já fez o restante da linha é o comando para invocar. No nosso exemplo, nós temos assegurado que o PAP a autenticação é necessária, CHAP com deficiência, e especificou que o sistema *passwd* arquivo deve ser usado para autenticando usuários. Este é provavelmente semelhante ao que você deseja. Lembre-se, você pode especificar as opções na *opções* arquivo ou na linha de comando, se preferir.

Aqui está uma pequena lista de tarefas a executar e na seqüência, você deve executá-las para obter discagem PPP no trabalho ção em sua máquina. Certifique-se de cada etapa de obras antes de passar para os próximos:

1. Configurar o modem para o modo de resposta automática. Em modems Hayes-compatible, este é realizado através de um comando como `ATS0 = 3`. Se você vai estar usando o `mgetty` daemon, isso não é necessário.

2. Configure o dispositivo de série com um `getty` tipo de comando para atender as chamadas. Um comumente usados `getty` variante é `mgetty`.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

3. Considere autenticação. Será que seu interlocutor autenticar usando o PAP, CHAP ou de login do sistema?

58 A `useradd` ou `adduser` utilidade, se tiver, vai simplificar esta tarefa.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

4. Configurar `pppd` como servidor, conforme descrito nesta seção.

5. Considere roteamento. Será preciso fornecer uma rota de rede para os chamadores? O roteamento pode ser realizada utilizando
o *ip-up* script.

Demanda de discagem

Quando há tráfego IP para ser efectuada através do link, *a marcação a pedido* faz com que seu modem de telefone para discar e estabelecer uma conexão com um host remoto. discagem por demanda é mais útil quando você não pode deixar sua linha telefônica
permanentemente ligado ao seu provedor de Internet. Por exemplo, você pode ter que pagar cronometrado chamadas locais, de modo que
pode ser mais barato para ter a linha de telefone ligado apenas quando você precisar dele e desconectada quando você não estão usando a Internet.

As soluções tradicionais de Linux têm usado o `diald` comando, que funcionou bem, mas foi bastante complicado para configure. As versões 2.3.0 e posterior do daemon PPP tem suporte embutido para marcação da procura e tornam muito simPLE para configurar. Você deve usar um kernel moderno para que isso funcione, também. Qualquer um dos kernels 2.0 mais tarde irá funcionar apenas
coima.

Para configurar `pppd` para a marcação a pedido, tudo que você precisa fazer é adicionar as opções para o seu *opções* arquivo ou o `pppd` comlinha de mando. A tabela abaixo resume as opções relacionadas com a demanda de discagem:

Opção	Descrição
`demanda`	Esta opção especifica que a ligação PPP deve ser colocado em modo de discagem por demanda. O PPP dispositivo de rede será criado, mas o `contato` comando não deverá ser utilizado até uma datagrama é transmitido pelo host local. Esta opção é obrigatória para a marcação a pedido para o trabalho.
`ativo-filtro` *expressão*	Esta opção permite que você especifique quais pacotes de dados devem ser consideradas tráfico activo fic. Qualquer tráfego correspondente a regra especificada será reiniciado o timer de discagem por demanda ociosa, assegurar que `pppd` espere novamente antes de fechar o link. A sintaxe do filtro foi emprestada do `tcpdump` comando. O filtro padrão corresponde a todos os datagramas.
`Holdoff` *n*	Esta opção permite que você especifique o montante mínimo de tempo, em segundos, para aguardar antes de reconectar esta ligação se encerra. Se a conexão falhar enquanto `pppd` serlieves ele está em uso ativo, ele será restabelecida após este temporizador expirou. Este temporizador não se aplica às religações após um período de inactividade.
`inativo` *n*	Se esta opção for configurada, `pppd` irá desligar a ligação, sempre que este timer expira. Inatividade são especificados em segundos. Cada novo pacote de dados ativa zerar o cronômetro.

Um simples pedido de marcação de configuração, portanto, algo parecido com isto:

```
demanda
Holdoff 60
idle 180
```

Esta configuração permitirá marcação a pedido, aguarde 60 segundos antes de restabelecer uma falha na conexão, e soltar o link se 180 segundo passar sem quaisquer dados ativo no link.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Persistente discagem

Marcação Persistentes é o que as pessoas que têm conexões dial-up permanente a uma rede que deseja usar. Não há uma sutil diferença entre a marcação ea marcação demanda persistente. Com a marcação persistente, a ligação é estabelecida automaticamente assim que a PPP daemon é iniciado, eo aspecto persistente entra em jogo quando,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

nunca, a chamada telefónica de apoio a ligação falhar. Marcação persistente garante que a ligação está sempre disponível
automaticamente reconstruir a conexão se ele falhar.

Você pode ter a sorte de não ter que pagar para os seus telefonemas, talvez eles são locais e livre, ou talvez eles são pagos pela sua empresa. A opção de discagem persistente é extremamente útil nesta situação. Se você tem para pagar os seus telefonemas, então você tem que ser um pouco cautelosos. Se você paga por suas chamadas telefônicas em um tempo
cobrado com base, discagem persistente quase certamente não é o que você quer, a menos que você tenha muita certeza você vai estar usando o
conexão quase constantemente 24 horas por dia. Se você não pagar por chamadas, mas não são cobrados o tempo, você precisa ter cuidado para proteger-se contra situações que possam causar o modem para remarcar interminavelmente. A `pppd` daemon fornece uma opção que pode ajudar a reduzir os efeitos deste problema.

Para ativar a discagem persistente, você deve incluir o *persistir* opção em um de seus `pppd` arquivos de opções. Incluindo esta opção só é tudo que você precisa ter `pppd` automaticamente chamar o comando especificado pela *contato* opção para reconstruir a conexão quando a ligação falhar. Se você está preocupado com o modem remarcação muito rapidamente (em
caso de falha do servidor ou do modem na outra extremidade da conexão), você pode usar o *Holdoff* opção para definir o montante mínimo de tempo que `pppd` vai esperar antes de tentar se reconectar. Esta opção não irá resolver o proble-
blema de uma falha custando-lhe dinheiro em telefonemas desperdiçada, mas ele vai pelo menos servir para reduzir o impacto de um.

Uma configuração típica pode ter persistentes opções de marcação que se parecem com isto:

```
persistir
Holdoff 600
```

O tempo de espera é especificado em segundos. No nosso exemplo, `pppd` espera um total de cinco minutos antes, após a remarcação
a chamada cai.

É possível combinar a marcação persistente com a marcação da demanda, utilizando *inativo* para soltar o link se estiver ociosa por
um período de tempo especificado. Nós duvidamos que muitos usuários gostariam de fazê-lo, mas este cenário é descrito brevemente na
`pppd` página do manual, se você gostaria de persegui-lo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 9 - TCP / IP Firewall

A segurança é cada vez mais importante para as empresas e indivíduos. O Internet forneceu-lhes um poderosa ferramenta para distribuir informações sobre si próprios e obter informações de outras pessoas, mas também tem ex-colocados los para os perigos que eles têm sido isentos. Computador crime, roubo de informações e danos maliciosos são todos os perigos potenciais.

Uma pessoa não autorizada e sem escrúpulos, que obtém acesso a um sistema de computador podem adivinhar senhas do sistema ou explorar os bugs e comportamento idiossincrático de determinados programas para obter uma conta de trabalho na máquina. Uma vez que eles são capazes de fazer logon no computador, eles podem ter acesso a informações que podem ser prejudiciais, tais como informações comercialmente sensíveis, como planos de marketing, novos detalhes do projeto, ou bancos de dados de informações do cliente.
Danificar ou modificar este tipo de dados pode causar prejuízos graves para a empresa.

A maneira mais segura para evitar danos generalizados como é para evitar que pessoas não autorizadas tenham acesso à rede para a máquina. Este é o lugar onde firewalls vêm dentro

AVISO: Construindo firewalls seguro é uma arte. Trata-se de um bom entendimento de tecnologia, mas também importante, que exige uma compreensão da filosofia por trás do firewall projetos. Nós não vamos cobrir tudo você precisa saber neste livro, nós recomendamos que você faça algumas pesquisas adicionais antes de confiar em qualquer design firewall particular, incluindo as que apresentamos aqui.

Há bastante material sobre configuração de firewall e design para encher um livro inteiro, e de fato há alguns bons recursos que você pôde gostar de ler para expandir seus conhecimentos sobre o assunto. Duas delas são:

Internet Firewalls Construindo

por D. Chapman e Zwicky E. (O'Reilly). Um guia que explica como criar e instalar firewalls para Unix, Linux e Windows NT, e como configurar os serviços de Internet para trabalhar com os firewalls.

Firewalls e Segurança na Internet

por W. Cheswick e S. Bellovin (Addison Wesley). Este livro aborda a filosofia de design do firewall e implementação.

Vamos nos concentrar nas questões específicas do Linux técnica neste capítulo. Posteriormente, vamos apresentar um firewall amostra con-figuração que deve servir como ponto de partida para a sua própria configuração, mas como com todos os relacionados à segurança assuntos, confiar em ninguém. Verifique o design, certifique-se de compreendê-lo e modificá-lo para atender às suas re-requisitos. Para ser seguro, ter a certeza.

Métodos de ataque

Como um administrador de rede, é importante que você compreenda a natureza dos possíveis ataques em segu-computador rança. Vamos descrever brevemente os mais importantes tipos de ataques de modo que você possa entender melhor o que exatamente o Linux firewall IP irá protegê-lo contra. Você deve fazer algumas leituras adicionais para garantir que você é capaz para proteger a rede contra outros tipos de ataques. Aqui estão alguns dos métodos mais importantes de ataque e as formas de proteger-se contra eles;

Acesso não autorizado

Isto significa simplesmente que as pessoas que não devem usar os seus serviços de computador são capazes de conectar e usar elas. Por exemplo, pessoas de fora da empresa pode tentar se conectar ao seu ma de contabilidade empresa chine ou para o servidor NFS.

Existem várias maneiras para evitar este ataque cuidadosamente, especificando quem pode ter acesso através dessas serviços. Você pode impedir o acesso à rede para todos, exceto os usuários pretendidos.

Exploração dos pontos fracos conhecidos em programas

Alguns programas e serviços de rede não foram originalmente concebidos com forte segurança em mente e são inerentemente vulnerável a ataques. Os serviços BSD remoto (rexec, rlogin, etc) são um exemplo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A melhor maneira de se proteger contra esse tipo de ataque é desativar todos os serviços vulneráveis ou encontrar alternativas. Com código aberto, às vezes é possível reparar os pontos fracos do software.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A negação de serviço

Ataques de negação de serviço que o serviço ou programa pare de funcionar ou impedir outros de fazer qualquer ing uso do serviço ou programa. Estes podem ser realizadas na camada de rede através do envio de cuidado datagramas criados e malicioso que causa as conexões de rede falhar. Podem também ser realizados em a camada de aplicação, onde os comandos da aplicação cuidadosamente trabalhada é dado a um programa de causa que tornar-se extremamente ocupado, ou parar de funcionar.

Impedindo o tráfego de rede suspeito de atingir os seus anfitriões e prevenir programa suspeito comandos e as solicitações são as melhores maneiras de minimizar o risco de um ataque de negação de serviço. É útil conhecer os detalhes do método de ataque, então você deve educar-se sobre cada novo ataque como fica divulgado.

Spoofing

Este tipo de ataque faz com que um host ou aplicativo para imitar as acções dos outros. Normalmente, o atacante finge ser um anfitrião inocentes seguintes endereços IP em pacotes de rede. Por exemplo, um bem-documentados explorar do serviço rlogin BSD pode usar esse método para simular uma conexão TCP a partir de um-outro host, adivinhando números de seqüência TCP.

Para se proteger contra esse tipo de ataque, verificar a autenticidade de datagramas e comandos. Previna-dados grama de roteamento com o endereço de origem inválido. Introduzir mecanismos de controlo unpredictablility em conexão
mos, tais como números de seqüência TCP e da atribuição de endereços de porta dinâmica.

Espionagem

Este é o tipo mais simples de ataque. Um host é configurado para "ouvir" e captação de dados não pertencentes ao ele. programas de espionagem cuidadosamente escrito pode ter nomes de usuário e senhas de login do usuário-rede relações de trabalho. As redes de televisão como Ethernet são especialmente vulneráveis a este tipo de ataque.

Para se proteger contra esse tipo de ameaça, evitar o uso de tecnologias de rede de transmissão e forçar o uso de criptografia de dados.

firewall IP é muito útil para prevenir ou reduzir o acesso não autorizado, a negação da camada de rede do serviço, e ataques spoofing IP. Ele não é muito útil para evitar a exploração de falhas nos serviços de rede ou de programas e de escutas.

O que é um Firewall?

Um firewall é uma máquina segura e confiável que fica entre uma rede privada e uma rede pública.[59] O fogo-máquina de parede é configurada com um conjunto de regras que determinam qual o tráfego de rede será permitida a passagem e que serão bloqueados ou recusados. Em algumas organizações de grande porte, você pode até achar um firewall localizados dentro de suas
rede corporativa para segregar áreas sensíveis da organização de outros funcionários. Muitos casos de com-putador crime ocorrer a partir de dentro de uma organização, não apenas do exterior.

Firewalls podem ser construídos completamente em uma variedade de maneiras. O arranjo mais sofisticado envolve um número de máquinas distintas e é conhecido como um *rede de perímetro*. Duas máquinas funcionam como "filtros" engasga chamado para permitir
apenas determinados tipos de tráfego de rede para passar, e entre estas bobinas residem os servidores de rede, como um e-mail gateway ou um servidor de World Wide Web Proxy. Essa configuração pode ser muito seguro e fácil permite uma grande grande gama de controle sobre quem pode se conectar tanto do interior para o exterior e do exterior para o interior. Este tipo de configuração pode ser utilizada por grandes organizações.

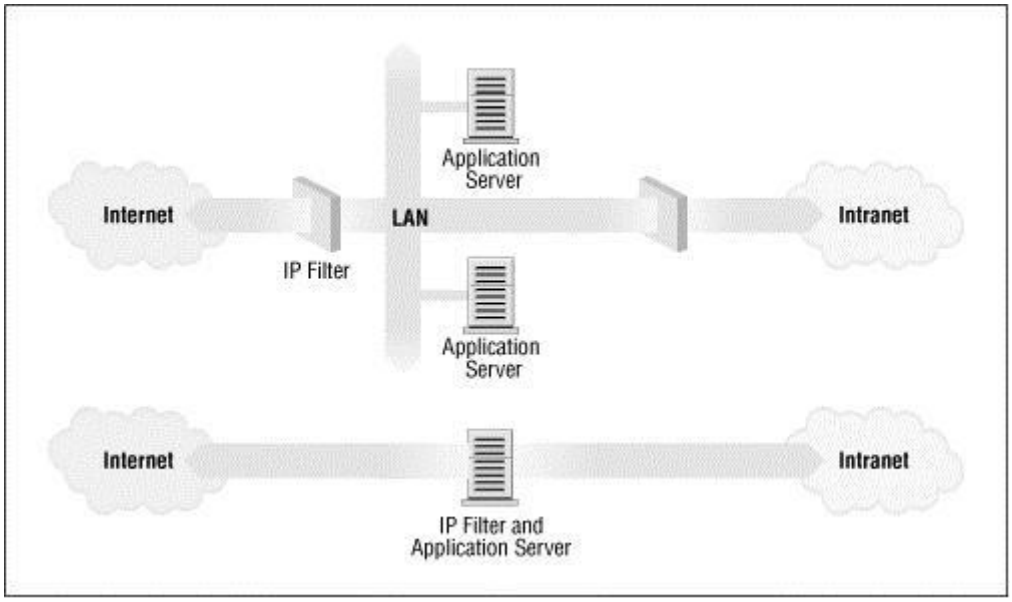
Normalmente, porém, os firewalls são únicas máquinas que servem todas essas funções. Estes são um pouco menos seguro, porque se houver alguma fraqueza na máquina firewall próprio que permite às pessoas ter acesso a ele, o conjunto segurança de rede foi rompida. No entanto, estes tipos de firewalls são mais baratas e fáceis de gerenciar que o arranjo mais sofisticado que acabamos de descrever. Figura 9.1 illudemonstra as duas configurações de firewall mais comum-rações.

---

[59] O termo *firewall* vem de um dispositivo usado para proteger as pessoas de fogo. O firewall é um escudo de material resistente ao fogo que é colocado entre um potencial de incêndio e as pessoas que ele está protegendo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Figura 9.1: As duas classes principais de design de firewall



O kernel Linux fornece uma gama de funcionalidades incorporadas que lhe permitem funcionar muito bem como um firewall IP.

A
implementação da rede inclui o código para fazer filtragem de IP em um número de diferentes maneiras, e fornece um mecanismo de forma bastante precisa configurar o tipo de regras que você gostaria de colocar no lugar. O firewall do Linux é flexível suficiente para torná-lo muito útil em qualquer uma das configurações ilustradas na Figura 9.1. Lisoftware de firewall nux fornece duas outras características úteis que vamos discutir em capítulos separados: IP Contabilidade (Capítulo 10, *IP Accontagem*) E IP Masquerade (Capítulo 11, *IP Masquerade e Network Address Translation*).

Qual é a filtragem de IP?

Filtragem de IP é simplesmente um mecanismo que decide quais os tipos de pacotes IP serão processados normalmente e que serão descartados. Por *descartados* queremos dizer que o datagrama é suprimida e completamente ignorado, como se tivesse nunca foi recebido. Você pode aplicar muitos tipos diferentes de critérios para determinar quais datagramas quiser filtro, alguns exemplos são:

- Tipo de protocolo: TCP, UDP, ICMP, etc
- Tomada de número (por TCP / UPD)
- Datagram tipo: SYN / ACK, dados, solicitação de eco ICMP, etc
- Datagram endereço de origem: de onde veio
- Datagram endereço de destino: para onde vai a

É importante entender nesse ponto que a filtragem IP é um mecanismo de camada de rede. Isto significa que não subsuportar qualquer coisa sobre o aplicativo usando as conexões de rede, apenas sobre as conexões se. Para exemplo, você pode negar o acesso dos usuários à rede interna na porta telnet padrão, mas se você confiar em IP filtragem sozinho, você não pode impedi-los de usar o programa telnet com uma porta que você deixe passar trhough seu firewall. Você pode evitar este tipo de problema usando servidores proxy para cada serviço que você permitir que toda a seu firewall. Os servidores proxy compreender a aplicação, foram concebidas para proxy e pode, portanto, prevent abusos, tais como a utilização do programa Telnet para obter um firewall passado usando a World Wide Web porta. Se a sua
firewall suporta uma World Wide Web proxy, a conexão telnet será sempre respondida pelo proxy e vai permitir que os pedidos só HTTP para passar. Um grande número de programas de servidor proxy existe. Alguns são de software livre
e muitos outros produtos comerciais. O Firewall-HOWTO discute um conjunto popular deles, mas eles estão fora do escopo deste livro.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O conjunto de regras de filtragem de IP é composto de muitas combinações dos critérios listados

anteriormente. Por exemplo, vamos
Imagine que você queria permitir que os usuários da World Wide Web na rede Cervejaria Virtual não tem acesso à Internet, exceto para usar servidores de outros sites da web. Você poderia configurar o firewall para permitir o encaminhamento de:

- datagramas com endereço de origem na rede virtual Brewery, um endereço de destino de qualquer lugar, e com uma porta de destino de 80 (WWW)
- datagramas com um endereço de destino da rede virtual cervejaria e uma porta de origem de 80 (WWW) de um endereço de origem de qualquer lugar

Note que usamos duas regras aqui. Temos que permitir que os nossos dados para sair, mas também os dados de resposta

correspondente
voltar polegadas Na prática, como veremos em breve, Linux e simplifica este nos permite especificar isso em um comando.

Configurando o Linux para Firewalling

Para construir um firewall Linux IP, é necessário ter um kernel compilado com suporte a IP firewall eo adequado Configuration Utility. Em toda a produção de grãos antes da série 2.2, você usaria o `ipfwadm` utilidade. A kernels 2.2.x marcou o lançamento da terceira geração do IP firewall para Linux chamado *IP Chains*. Redes IP usam um programa semelhante ao `ipfwadm` chamada `ipchains`. kernels Linux 2.3.15 e posteriores oferecem suporte a quarta geração de
Linux firewall IP chamado *netfilter*. A *netfilter* código é o resultado de um grande redesenho do fluxo de movimentação de pacotes em
Linux. A *netfilter* é uma criatura multifacetada, fornecendo suporte retrocompatível directo para ambos `ipfwadm` e `ipchains` bem como uma nova alternativa de comando chamado `iptables`. Vamos falar sobre as diferenças setre os três próximas seções.

Kernel configurado com IP Firewall

O kernel do Linux deve ser configurado para suportar o firewall IP. Não há muito mais do que selecionando o opções apropriadas ao realizar uma `make menuconfig` de seu kernel.[60] Nós descrevemos como fazer isso está em Capítulo 3, *Configurando o hardware de rede*. "No kernel 2.2 você deve selecionar as seguintes opções:

```
Networking options  --->
        [*] Os firewalls de rede
        [*] Rede TCP / IP
        [*] IP: firewall
        [*] IP: firewall packet logging
```

Nos kernels 2.4.0 e depois você deve selecionar essa opção em vez disso:

```
  Networking options  --->
     [*] Network packet filtering (substitui o ipchains)
         IP: Netfilter Configuration  --->
              .
             <M> Userspace filas através NETLINK (EXPERIMENTAL)
             <M> IP suporta tabelas (necessário para a filtragem / masc / NAT)
             <M>   match limit apoio
             <M>   Apoio MAC corresponde ao endereço
             <M>   apoio partida netfilter MARK
             <M>   O suporte a múltiplos jogo porto
             <M>   TOS jogo apoio
             <M>   Conexão apoio partida Estado
             <M>   Imundo apoio de jogo (EXPERIMENTAL)
             <M>   Proprietário apoio de jogo (EXPERIMENTAL)
             <M>   A filtragem de pacotes
             <M>     apoio alvo REJECT
             <M>     Espelho para alvo (EXPERIMENTAL)
              .
             <M> Packet desconfiguração
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

60 Firewall pacote de log é um recurso especial que escreve uma linha de informações sobre cada datagrama que corresponde a uma regra de firewall particular para um dispositivo especial para que você possa vê-las.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
<M>     TOS apoio alvo
<M>     MARK apoio alvo
<M>   LOG apoio alvo
ipchains <M> (2,2-style) de apoio
<M> Ipfwadm (2.0-style) de apoio
```

O utilitário ipfwadm

A `ipfwadm` (IP Firewall Administration) utilidade é a ferramenta usada para construir as regras do firewall para todos os kernels anteriores
a 2.2.0. Sua sintaxe de comando pode ser muito confuso, porque ele pode fazer uma gama tão complicado de coisas, mas vamos dar alguns exemplos comuns que irão ilustrar as variações mais importantes destes.

A `ipfwadm` utilitário está incluído na maioria das distribuições Linux modernas, mas talvez não por padrão. Pode haver um pacote de software específico para isso que você tem que instalar. Se sua distribuição não inclui-lo, você pode obter o pacote de fonte de *ftp.xos.nl* na */ Pub / linux / ipfwadm /* diretório, e compilá-la.

O utilitário ipchains

Assim como para o `ipfwadm` utilidade, o `ipchains` utilitário pode ser um pouco desconcertante para usar em primeiro lugar.

Ela possibilita que todos
a flexibilidade de `ipfwadm` com uma sintaxe de comandos simplificados, e, adicionalmente, fornece um mecanismo de "encadeamento",
nismo que permite gerenciar múltiplos conjuntos de regras e vinculá-los. Nós vamos cobrir o encadeamento regra em separado ponto próximo ao final do capítulo, porque para a maioria das situações, é um conceito avançado.

A `ipchains` comando aparece na maioria das distribuições Linux baseado no kernel 2.2. Se você deseja compilar isso mesmo, você pode encontrar o pacote fonte do site do desenvolvedor na sua http://www.rustcorp.com/linux/ipchains/. Incluído no pacote fonte é um script chamado `ipfwadm-wrapper` que imita o `ipfwadm` comando, mas na verdade chama o `ipchains` comando. A migração de uma configuração de firewall existente seja muito mais fácil com este aditamento.

O utilitário iptables

A sintaxe da `iptables` utilitário é bastante semelhante ao do `ipchains` sintaxe. As mudanças são im-
melhorias e resultado da ferramenta que está sendo redesenhado para ser extensível através de bibliotecas compartilhadas. Assim como para `ip-cadeias`, Vamos apresentar `iptables` equivalentes dos exemplos que você possa comparar e contrastar com sua sintaxe os outros.

A `iptables` utilitário está incluído no *netfilter* pacote de fontes disponíveis no http://www.samba.org/netfilter/.É também será incluído em qualquer distribuição Linux baseada no kernel 2.4 série.

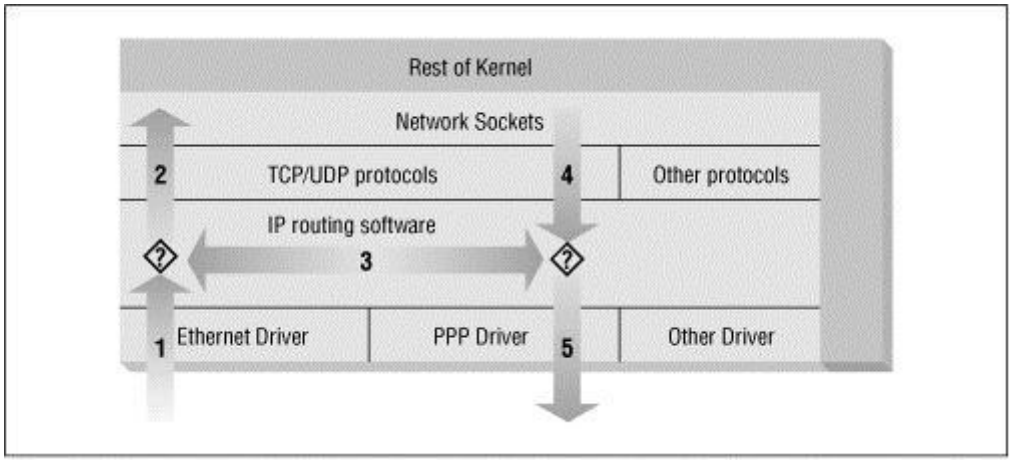
Vamos falar um pouco sobre *netfilter*É enorme passo em frente em uma seção própria, mais adiante neste capítulo.

Três maneiras que nós podemos fazer a filtragem

Considere como uma máquina Unix, ou de facto qualquer máquina capaz de roteamento IP, os processos de datagramas IP. O básico
etapas, mostradas na Figura 9.2 são:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Figura 9.2: Os estágios de processamento de datagramas IP



- O datagrama IP é recebida. (1)
- O datagrama IP de entrada é analisado para determinar se ele é destinado a um processo nesta

máquina.

- Se o datagrama é para esta máquina, ela é processada localmente. (2)
- Se não for destinada para esta máquina, uma pesquisa é feita da tabela de roteamento para uma rota adequada e o datagrama é encaminhado para a interface apropriada ou descartada se nenhuma rota pode ser encontrado. (3)
- Datagramas de processos locais são enviados para o software de roteamento para encaminhamento ao respectivo inter-rosto. (4)
- O datagrama IP de saída é examinado para determinar se existe uma rota válida para ele tomar, se não, é caiu.
- O datagrama IP é transmitida. (5)

Em nosso diagrama, o fluxo 1 3 5 representa a nossa máquina de roteamento de dados entre um host na nossa rede Ethernet para um host alcançável através do nosso link PPP. Os fluxos de 1, 2 e 4 5 representam a entrada de dados e fluxos de saída de um líquido,
programa de trabalho em execução no nosso host local. O fluxo 4 3 2 representaria o fluxo de dados através de uma conexão de loopback.
Naturalmente, ambos os fluxos de dados de entrada e saída de dispositivos de rede. Os pontos de interrogação no diagrama representam os
pontos onde a camada IP toma decisões de roteamento.

O kernel do Linux firewall IP é capaz de aplicar filtragem em várias fases deste processo. Ou seja, você pode filtrar os datagramas IP que vêm em sua máquina, filtrar os datagramas sejam enviados através de sua ma-chine e filtrar os datagramas que estão prontos para serem transmitidos.

Em `ipfwadm` e `ipchains`, Uma regra de entrada aplica-se a um fluxo no diagrama, uma regra de encaminhamento de fluxo 3,

e
uma regra de saída para o fluxo 5. Vamos ver quando discutimos *netfilter* depois que os pontos de intercepção mudaram tão que uma regra de entrada é aplicado no fluxo de O 2, e uma regra de saída é aplicada ao fluxo 4. Isto tem implicações importantes para
como você estrutura seu conjuntos de regras, mas o princípio geral é válido para todas as versões do firewall Linux.

Isto pode parecer desnecessariamente complicado no início, mas oferece uma flexibilidade que permite que alguns muito

sofisticados
e as configurações poderosas a ser construído.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Original Firewall IP (kernels 2.0)

A primeira geração do suporte a firewall IP para Linux apareceu no kernel série 1.1. Era um porto do ipfw do BSD suporte a firewall para o Linux por Alan Cox. O suporte a firewall que apareceu na série de kernels 2.0 e é o da segunda geração foi melhorada por Jos Vos, Pauline Middelink, entre outros.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Usando ipfwadm

A `ipfwadm` comando foi a ferramenta de configuração para a geração Linux segunda firewall IP. Talvez o
maneira mais simples de descrever o uso do `ipfwadm` comando é pelo exemplo. Para começar, vamos codificar o exemplo que apresentado anteriormente.

Um exemplo ingênuo

Vamos supor que temos uma rede em nossa organização e que nós estamos usando uma máquina de firewall baseado em Linux para conectar a nossa rede à Internet. Além disso, vamos supor que nós desejamos que os usuários dessa rede a ser
capaz de acessar os servidores web na internet, mas permitir que nenhum outro tráfego a serem passados.

Vamos pôr em prática uma regra para permitir o encaminhamento de datagramas com endereço de origem em nossa rede e um

destino,
Tomada ção de porta 80 para ser enviado para fora, e para os datagramas respectiva resposta deverão ser enviadas de volta por meio
o firewall.

Assumir nossa rede tem uma máscara de rede 24 bits (classe C) e um endereço de 172.16.1.0. As regras que podemos usar são:

```
#  Ipfwadm-F-f
#  ipfwadm-F-p deny
#  Ipfwadm-F-a accept-P tcp-S 172.16.1.0/24-D 0 / 0 80
#  Ipfwadm-F-a accept-P tcp-S 0 / 0 172.16.1.0/24 80-D
```

A *-F* argumento de linha de comando diz `ipfwadm` que esta é uma regra de encaminhamento. O primeiro comando instrui `ipfwadm` para "lavar" todas as regras de encaminhamento. Isso garante que estamos a trabalhar a partir de um estado conhecido antes
começar a adicionar regras específicas.

A segunda regra define a nossa política de encaminhamento padrão. Nós dizemos que o kernel para negar ou impedir transmissão de dados em

IP
gramas. É muito importante para definir a política padrão, pois este descreve o que vai acontecer com os datagramas que não sejam especificamente tratados por qualquer outra regra. Na maioria das configurações de firewall, você vai querer definir o seu
política padrão para "negar", como mostrado, para ter certeza de que somente o tráfego que você permitir especificamente o seu passado de firewall é
encaminhados.

As regras de terceira e quarta são os que implementam a nossa exigência. O terceiro comando permite que nossos dados gramas para fora, ea quarta regra permite que as respostas de volta.

Vamos analisar cada um dos argumentos:

-F

Esta é uma regra de encaminhamento.

-A aceitar

Acrescente esta regra com a política definida para "aceitar", o que significa que irá encaminhar os datagramas que corresponder a esse
regra.

-P tcp

Esta regra aplica-se a datagramas TCP (em oposição a UDP ou ICMP).

-S 172.16.1.0/24

O endereço de origem deve ter os primeiros 24 bits correspondentes às do endereço de rede 172.16.1.0.

D-0 / 0 80

O endereço de destino deve ter zero bits correspondente ao endereço 0.0.0.0. Este é realmente um atalho no-ção para "qualquer coisa". A 80 é a porta de destino, neste caso WWW. Você também pode usar qualquer entrada que aparece na */ Etc / services* arquivo para descrever a porta, de modo `Www-D 0 / 0` teria trabalhado como também.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`ipfwadm` aceita máscaras de rede em uma forma com a qual você pode não estar familiarizado. A `/ Nn` notação é um meio de descrevendo quantos bits do endereço fornecidos são significativos, ou o tamanho da máscara. Os bits são sempre contado da esquerda para direita, alguns exemplos mais comuns estão listados na Tabela 9.1.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Tabela 9.1: Máscara de rede Bit Valores Comuns

Netmask	Bits
255.0.0.0	8
255.255.0.0	16
255.255.255.0	24
255.255.255.128	25
255.255.255.192	26
255.255.255.224	27
255.255.255.240	28
255.255.255.248	29
255.255.255.252	30

Mencionamos anteriormente que `ipfwadm` implementa um pequeno truque que faz a adição destes tipos de regras mais fácil. Este
truque é uma opção chamada *-B*, O que torna o comando regra bidirecional.

A bandeira bidirecional permite-nos recolher as nossas duas regras em uma como segue:

```
# Ipfwadm-F-a accept-P tcp-S 172.16.1.0/24-D 0 / 0 80-b
```

Um refinamento importante

Dê uma olhada no nosso conjunto de regras. Você pode ver que há ainda um método de ataque que fora alguém poderia usar para derrotar nosso firewall?

Nosso conjunto de regras permite que todos os datagramas de fora da nossa rede com uma porta de origem 80 para passar. Isto incluirá
os datagramas com o bit SYN definido! O bit SYN é o que declara um datagrama TCP é um pedido de conexão.
Se uma pessoa do lado de fora tinha um acesso privilegiado a um host, eles poderiam fazer uma conexão através de nosso firewall para
qualquer um dos nossos anfitriões, desde que utilizem a porta 80 em sua extremidade. Este não é o que pretendemos.

Felizmente há uma solução para este problema. A `ipfwadm` comando fornece uma outra bandeira que nos permite
criar regras que irá corresponder datagramas com o bit SYN. Vamos mudar o nosso exemplo para incluir essa regra:

```
# Ipfwadm-F-a deny-P tcp-S 0 / 0 80-D 172.16.10.0/24-y
# Ipfwadm-F-a accept-P tcp-S 172.16.1.0/24-D 0 / 0 80-b
```

A *-Y* sinalizador faz com que a regra a correspondência apenas se a flag SYN está situado no datagrama. Portanto, a nossa nova regra diz: "Negar qualquer
TCP datagramas destinados a nossa rede de qualquer lugar com uma porta de origem 80 eo conjunto de bits SYN ", ou" Negar todos os pedidos de conexão de hosts usando a porta 80. "

Por que temos colocado esta regra especial *antes* a principal regra? regras de firewall IP funcionar de forma que o primeiro jogo é o
regra que é usada. Ambas as regras que correspondem os datagramas queremos parar, então nós devemos ter a certeza de colocar o `negar`
Estado antes da `aceitar` regra.

Listagem de nossas regras

Depois entramos nossas regras, nós pedimos `ipfwadm` listá-las para nós usando o comando:

```
# Ipfwadm-F-l
```

Este comando vai listar todas as regras de encaminhamento configurado. A saída deve ser algo parecido com isto:

```
# Ipfwadm-F-l
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
firewall IP regras para a frente, a política padrão: aceitar
tipo  fonte prot                destino              portas
negar tcp  em qualquer lugar    172.16.10.0/24       www -> qualquer outro
acc   tcp  172.16.1.0/24        em qualquer lugar    qualquer - www>
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A `ipfwadm` comando tentativa de traduzir o número da porta em um nome de serviço usando o */ Etc / services* se existe uma entrada lá.

A saída padrão é falta de algum detalhe importante para nós. Na saída de listagem padrão, não podemos ver o efeito da `-Y` argumento. A `ipfwadm` comando é capaz de produzir uma saída de lista mais detalhada se você especificar o `-E` (Saída estendida), argumento também. Não vamos mostrar toda a produção aqui, porque é demasiado ampla para a página, mas inclui uma `opt` (Opções) que mostra a coluna *-Y* opção de controle de pacotes SYN:

```
# ipfwadm-F-l e-
P regras de firewall para a frente, a política padrão: aceitar
 tipo pkts bytes  prot opt  ifname tosa tosx  ifaddress   fonte          ...
    0     0 negar tcp  - 0x00-0xff qualquer y qualquer    em qualquer    ...
                                                          lugar
    0     0 acc   tcp  b --- 0xff 0x00        qualquer    172.16.1.0/24 ...
          qualquer
```

Um exemplo mais complexo

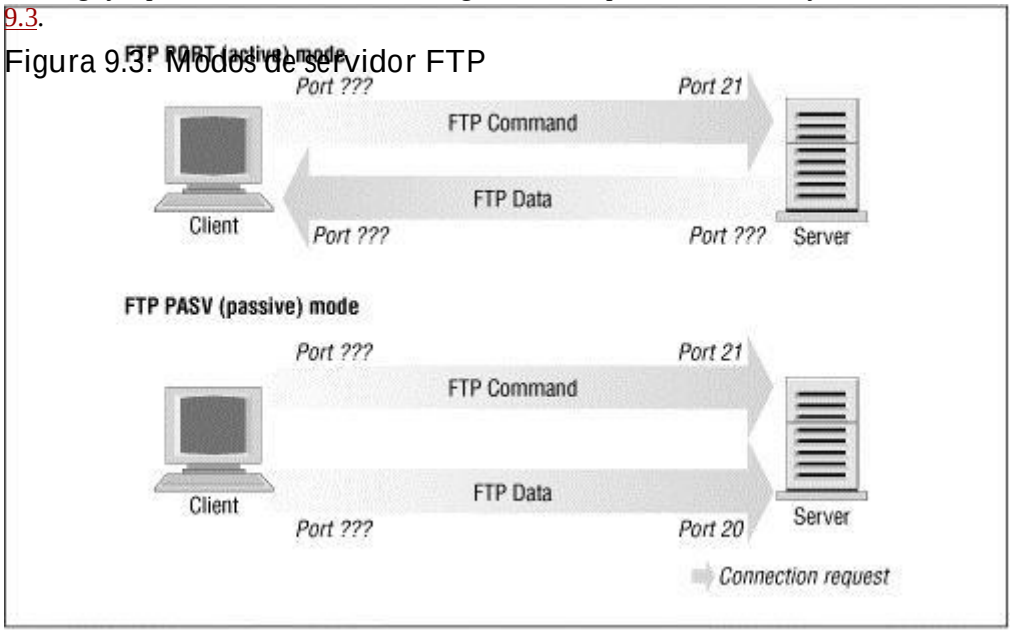
O exemplo anterior foi simples. Nem todos os serviços de rede são tão simples como o serviço WWW para config-
Ure, na prática, uma configuração de firewall típico seria muito mais complexa. Vejamos outro comum
exemplo, desta vez de FTP. Queremos que os nossos utilizadores da rede interna para poder entrar em servidores de FTP na Internet para
ler e escrever arquivos. Mas nós não queremos que as pessoas na internet para ser capaz de entrar em nossos servidores de FTP.

Sabemos que o FTP usa duas portas TCP: port 20 (ftp-data) ea porta 21 (ftp), então:

```
# ipfwadm-a deny-P tcp-S 0 / 0 20-D 172.16.1.0/24-y
# ipfwadm-a accept-P tcp-S 172.16.1.0/24-D 0 / 0 20-b
#
# ipfwadm-a deny-P tcp-S 0 / 0 21-D 172.16.1.0/24-y
# ipfwadm-a accept-P tcp-S 172.16.1.0/24-D 0 / 0 21-b
```

Certo? Bem, não necessariamente. servidores de FTP pode operar em dois modos diferentes: modo passivo e modo ativo.[61] No modo passivo, o servidor FTP escuta para uma conexão do cliente. No modo ativo, o servidor realmente faz a ligação para o cliente. modo activo é geralmente o padrão. As diferenças são ilustradas na Figura 9.3.

Figura 9.3: Modos de servidor FTP



Muitos servidores FTP fazer sua conexão de dados da porta 20 quando operando em modo ativo, o que simplifica coisas para nós um pouco, mas infelizmente não todos.[62]

61 FTP modo ativo é um pouco nonintuitively habilitado com o PORT comando. FTP em modo passivo é ativado, usando o PASV commando.

62 O daemon proftpd é um bom exemplo de um servidor de FTP que não, pelo menos em versões mais antigas.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Mas como isso nos afeta? Dê uma olhada em nossa regra para a porta 20, a porta FTP-data. A regra como temos agora assume que a conexão será feita pelo nosso cliente para o servidor. Isto irá funcionar se usar o modo passivo. Mas é muito difícil para nós, para configurar uma regra satisfatória para permitir que o FTP de modo ativo, porque não podemos saber em antecipadamente quais portas serão utilizadas. Se abrirmos o nosso firewall para permitir conexões de entrada em qualquer porto, estamos expor a nossa rede para atacar em todos os serviços que aceitam conexões.

O dilema é mais segura resolvido, insistindo em que nossos usuários operar em modo passivo. A maioria dos servidores FTP e muitos clientes FTP irá funcionar desta maneira. O popular `ncftp` cliente também suporta o modo passivo, mas pode require uma pequena alteração na configuração para torná-lo padrão para o modo passivo. Muitos navegadores da World Wide Web, tais como o navegador Netscape também suportam modo passivo de FTP, por isso não deve ser muito difícil de encontrar o software adequado uso. Alternativamente, você pode evitar o problema inteiramente ao usar um servidor proxy FTP que aceita uma conexão de a rede interna e estabelece conexões com a rede externa.

Na construção de seu firewall, você provavelmente vai encontrar um número desses tipos de problemas. Você deve sempre dar cuidado pensamento a como um serviço realmente funciona para ter certeza de ter posto em prática um conjunto de regras adequadas para isso. A configuração de firewall real pode ser bastante complexo.

Resumo dos argumentos ipfwadm

A `ipfwadm` tem muitos argumentos diferentes que se relacionam com a configuração do firewall IP. A sintaxe geral é:

`ipfwadm` *categoria parâmetros de comando [opções]*

Vamos dar uma olhada em cada uma delas.

Categorias

Um e apenas um dos seguintes devem ser fornecidas. A categoria informa o firewall que tipo de regra de firewall que você está configurando:

-I
: regra de entrada

-O
: regra de saída

-F
: regra de encaminhamento

Comandos

Pelo menos um dos seguintes procedimentos devem ser fornecidos e se aplica somente a essas regras que se relacionam com a categoria fornecido.
O comando diz ao firewall que atitude tomar.

-A [política]
: Acrescentar uma nova regra

-I [política]
: Inserir uma nova regra

[Política] d
: Apagar uma regra em vigor

-P política
: Definir a política padrão

-L
: Lista de todas as regras existentes

-F

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Lave todas as regras existentes

As políticas relevantes para o firewall IP e seus significados são:

aceitar

Permite datagramas correspondência a ser recebida, enviada ou transmitida

negar

Blocos correspondentes datagramas sejam recebidas, enviadas ou transmitidas

rejeitar

Blocos correspondentes datagramas sejam recebidas, enviadas ou transmitidas, e envia o host que enviou o datagrama e mensagem de erro ICMP

Parâmetros

Pelo menos uma das seguintes opções devem ser fornecidas. Use os parâmetros para especificar a quais datagramas este ap-regra camadas:

-P protocolo

Pode ser TCP, UDP ICMP, ou todos. Exemplo:

```
-P tcp
```

-S address [/ mask] [porta]

Endereço IP de origem que essa regra irá corresponder. A máscara de "/ 32" será assumido se você não fornecer um. Você pode, opcionalmente, especificar quais as portas que esta regra será aplicada. Você também deve especificar o protocolo com
o *-P* argumento descrito acima para este trabalho. Se você não especificar um intervalo de portas ou porta, "todas" as portas
será assumido a combinar. As portas podem ser especificadas por nome, utilizando suas */ Etc / services* entrada, se desejar. Em
o caso do protocolo ICMP, o campo de porta é usada para indicar os tipos de datagramas ICMP. Porto intervalos pode ser descrito, use a sintaxe geral: *lowport*:*highport*. Aqui está um exemplo:

```
-S 172.29.16.1/24 ftp:ftp-data
```

D-address [/ mask] [porta]

Especifique o endereço IP de destino que essa regra irá corresponder. O endereço de destino é codificado com o mesmas regras que o endereço de origem descrita anteriormente. Aqui está um exemplo:

```
-D 172.29.16.1/24 smtp
```

V-endereço

Especifique o endereço da interface de rede na qual o pacote é recebido (*-I*) Ou está sendo enviado (*-O*).
Isto permite-nos criar regras que se aplicam somente às interfaces de rede certo na nossa máquina. Aqui está um exemplo:

```
-V 172.29.16.1
```

W-nome

Especifique o nome da interface de rede. Este argumento funciona da mesma forma como o *-V* argumento, exceto que você fornecer o nome do dispositivo, em vez de seu endereço. Aqui está um exemplo:

```
-W ppp0
```

Argumentos opcionais

Estes argumentos são às vezes muito úteis:

-B

Isto é usado para o modo bidirecional. Este sinalizador corresponde tráfego fluindo em ambos os sentidos entre os origem e destino especificados. Isso evita que você tenha que criar duas regras: uma para a frente di-
reção de uma ligação e outra para o inverso.

-O

Isso permite o registro de correspondência de datagramas para o log do kernel. Qualquer datagrama que corresponde a esta regra será
ser registrado como uma mensagem de kernel. Isso é útil para que você possa detectar o acesso não autorizado.

-Y

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

-K

Isto é usado para combinar datagramas TCP contato. A opção faz com que a regra para combinar datagramas apenas que
tentativa de estabelecer conexões TCP. Apenas os datagramas que têm suas bit SYN, mas a sua não-bit ACK definido, irá corresponder. Isso é útil para filtrar as tentativas de conexão TCP e é ignorado por outros protocolos.

Isto é usado para combinar datagramas TCP reconhecimento. Esta opção faz com que a regra para corresponder apenas datagramas que são reconhecimentos de pacotes tentam estabelecer conexões TCP. Somente dados
gramas que tenham o bit ACK irá corresponder. Isso é útil para filtrar as tentativas de conexão TCP e é ignored para todos os outros protocolos.

datagrama tipos ICMP

Cada um dos comandos de configuração de firewall permite que você especifique tipos datagrama ICMP. Ao contrário do TCP e

UDP
portos, não há nenhum arquivo de configuração conveniente que lista os tipos de datagrama e seus significados. Os dados ICMP tipos de grama são definidos no RFC-1700, o RFC Assigned Numbers. Os tipos de datagrama ICMP também estão listados no um dos arquivos de cabeçalho padrão C biblioteca. A */ Usr / include / netinet / ip_icmp.h* arquivo, que pertence ao GNU pacote da biblioteca padrão e é usado por programadores C, ao escrever o software de rede que utiliza o ICMP protocolo, também define os tipos de datagrama ICMP. Para sua comodidade, listamos-os em Tabela 9.2.A `IPT-veis` interface de comandos permite que você especifique tipos ICMP por nome, por isso, listamos os mnemônicos que utiliza, como também.

Tabela 9.2: Tipos de datagrama ICMP

Tipo Número	iptables Mnemonic	Descrição Tipo
0	resposta de eco-	Echo Reply
3	destino inalcançável	Destino inacessível
4	source-quench	Source Quench
5	redirecionar	Redirecionar
8	echo-request	Echo Request
11	tempo excedido	Time Exceeded
12	parâmetro-problema	Parâmetro Problema
13	timestamp pedido	Pedido Timestamp
14	timestamp-reply	Timestamp Responder
15	none	Pedido de Informação
16	none	Informações Responder
17	máscara de endereço-pedido	Endereço máscara pedido
18	máscara de endereço- resposta	Endereço máscara resposta

Correntes Firewall IP (kernels 2.2)

A maioria dos aspectos do Linux estão evoluindo para atender às crescentes demandas de seus usuários; firewall IP não é

exceção. A
implementação de firewall tradicional IP é bom para a maioria das aplicações, mas pode ser desajeitado e ineficiente para config-
ure para ambientes complexos. Para resolver este problema, um novo método de configurar o firewall IP e FEA-relacionadas turas foi desenvolvido. Este novo método foi chamado de "IP Firewall Chains" e foi lançado para uso geral em 2.2.0 do kernel do Linux.

O IP Firewall Chains foi desenvolvido por Paul Russell e Neuling Michael Rash e é mencionado a

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

63 Paulo pode ser alcançado em Paul.Russell rustcorp.com.au @.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

IP Firewall Chains permite-lhe desenvolver aulas de regras de firewall para o qual você pode então adicionar e remover hosts ou redes. Um artefato de regras de firewall encadeamento é que ela pode melhorar o desempenho em configurações de firewall em
que há muitas regras.

IP Firewall Chains são suportados pelo kernel 2.2 série e também estão disponíveis como um patch para a versão 2.0 .* ker-Nels. O tutorial descreve como obter o patch e fornece muitas dicas úteis sobre como efetivamente
usar o `ipchains` Configuration Utility.

Usando ipchains

Há duas maneiras que você pode usar o `ipchains` utilidade. A primeira maneira é fazer uso do `ipfwadm-invólucro` shell script, que é principalmente um substituto para `ipfwadm` que impulsiona o `ipchains` programa em segundo plano. Se você quiser fazer isso, então não leia mais. Em vez disso, releia as seções anteriores descrevem `ipfwadm`E substituto `ipfwadm-wrapper` em seu lugar. Isto irá funcionar, mas não há garantia de que o
script será mantida, e você não estará tomando partido de qualquer uma das características avançadas que o IP de fogo Cadeias de parede tem a oferecer.

A segunda forma de utilização `ipchains` é aprender a nova sintaxe e modificar todas as configurações existentes você tem que usar a nova sintaxe em vez do velho. Com cuidadosa consideração, você pode achar que você pode otimizar o seu configuração como converter. A `ipchains` sintaxe é mais fácil de aprender do que a `ipfwadm`, Então esta é uma boa opção.

A `ipfwadm` manipulado três conjuntos de regras com o objetivo de configurar o firewall. Com IP firewall chains
você pode criar números de forma arbitrária de conjuntos de regras, cada uma ligada a um outro, mas há três conjuntos de regras relacionadas com a
firewall que estão sempre presentes. Os conjuntos de regras padrão são equivalentes diretos desses usados com `ipfwadm`, exceto que eles têm nomes: `Entrada`,`frente` e `saída`.

Vamos primeiro na sintaxe geral do `ipchains` comando, então vamos olhar como nós usaríamos `ipchains`
em vez de `ipfwadm` sem se preocupar com qualquer uma das funcionalidades avançadas de encadeamento. Nós vamos fazer isso, revisitando
nossos exemplos anteriores.

Sintaxe de comando ipchains

A `ipchains` sintaxe deste comando é simples. Vamos agora olhar para o mais importante deles. O general
mais sintaxe `ipchains` comandos é:

`ipchains` *Opções do comando de especificação de regras*

Comandos

Há uma série de maneiras que podemos manipular as regras e conjuntos de regras com o `ipchains` comando. Aqueles

relevantes
para o firewall IP são:

-A cadeia

> Acrescente uma ou mais regras para a final da cadeia de nomeada. Se uma máquina é fornecida como uma ou outra fonte
> ou de destino e ele resolve para mais de um endereço IP, uma regra será adicionada para cada endereço.

-I cadeia rulenum

> Insira uma ou mais regras para o início da cadeia de nomeada. Novamente, se uma máquina é fornecida na regra especificação, uma regra será adicionada para cada um dos endereços que ele resolve.

-D cadeia

> Excluir uma ou mais regras da cadeia especificada que corresponda às especificações da regra.

-D chain rulenum

> Eliminar a regra que residem na posição *rulenum* na cadeia especificada. posições começam em um artigo para o primeiro

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

regra da cadeia.

-R chain rulenum

Substituir a regra que residem na posição *rulenum* na cadeia específica com a especificação fornecida regra.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

-C cadeia

Verifique o datagrama descrito pela especificação regra contra a corrente específica. Este comando retornar uma mensagem descrevendo como o datagrama foi processada pela cadeia. Isto é muito útil para o teste-ing sua configuração de firewall, e olhamos para ele em detalhes um pouco mais tarde.

-L [cadeia]

Listar as regras da cadeia especificada, ou para todas as cadeias se nenhuma corrente é especificada.

-F [chain]

Lave as regras da cadeia especificada, ou para todas as cadeias se nenhuma corrente é especificada.

-Z [cadeia]

Zerar os contadores de datagramas e de bytes para todas as regras da cadeia especificada, ou para todas as cadeias se nenhuma corrente é
especificado.

-N cadeia

Criar uma nova cadeia com o nome especificado. Uma cadeia de mesmo nome, não deve existir. Esta é como cadeias definidas pelo usuário são criados.

-X [cadeia]

Eliminar a cadeia definido pelo usuário, ou todas as chains definidas pelo usuário se não houver corrente é especificada.

Para este
comando para ser bem sucedido, não deve haver referências à cadeia especificada de quaisquer outras regras cadeia.

-P cadeia política

Definir a política padrão da cadeia especificada para a política especificada. as políticas de firewall são válidos `ACCEPT`,`NEGAR`,`REJECT`,`REDIR`Ou `RETORNO`.`ACCEPT`,`NEGAR`E `REJECT` têm os mesmos significados como aqueles para a implementação de firewall tradição IP. `REDIR` especifica que o datagrama deve ser transparente redirecionado para uma porta no host firewall. A `RETORNO` destino faz com que o código do IP firewall para
retornar à Cadeia Firewall que chamou a que contém esta regra e continua iniciando no af regra ter a regra de chamada.

especificação de parâmetros da regra

Um certo número de `ipchains` parâmetros de criar uma especificação de regra determinando que tipos de pacotes de partida.

Se
Cada um destes parâmetros é omitido uma especificação regra, o seu padrão é assumido:

-P [!] Protocolo

Especifica o protocolo de datagrama que irá corresponder a essa regra. nomes de protocolos válidos são `tcp`,`udp`, `icmp`Ou `todos`. Você também pode especificar um número de protocolo aqui para combinar outros protocolos. Por exemplo,
você pode usar `4` para coincidir com o `ipip` encapsulamento protocolo. Se o `!` é fornecido, a regra é negado e o datagrama irá corresponder a qualquer outro protocolo que o protocolo especificado. Se este parâmetro não for fornecido,
ele será o padrão para `todos`.

-S [!] Endereço [/ mask] [!] [Porta]

Especifica a fonte de endereço e porta do datagrama que correspondem a essa regra. O endereço pode ser sup-dobrado como um host, um nome de rede ou um endereço IP. O opcional `máscara` é a máscara para usar e pode ser fornecido sob a forma tradicional (por exemplo, / 255.255.255.0) ou a forma moderna (por exemplo, / 24). A opcional `porto` especifica a porta TCP ou UDP, ou o tipo de datagrama ICMP que irá corresponder. Você pode fornecer uma especificação de porta somente se você tiver fornecido o *-P* parâmetro com um dos `tcp`,`udp`Ou `icmp` protocolos. As portas podem ser especificadas como um conjunto, especificando o limite superior e inferior do intervalo com um
cólon como um delimitador. Por exemplo, `20:25` descritas todas as portas numeradas de 20 até e incluindo-ção 25. Novamente, o `!` personagem pode ser usado para negar os valores.

-D [!] Endereço [/ mask] [!] [Porta]

Especifica o endereço de destino ea porta do datagrama que irá corresponder a essa regra. A codificação deste

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

parâmetro é a mesma que a do *-S* parâmetro.

J-alvo

Especifica a ação a ser tomada quando esta regra encontrados. Você pode pensar desse parâmetro no sentido de "salto para. metas "válidos são `ACCEPT`,`NEGAR`,`REJECT`,`REDIR`E `RETORNO`. Descrevemos os significados de

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

cada uma dessas metas anteriores. No entanto, você também pode especificar o nome de uma chain definida pelo usuário, onde
processamento continuará. Se este parâmetro for omitido, nenhuma ação será tomada em datagramas regra correspondente na
todos os outros do que para atualizar os contadores de datagramas e de bytes.

-I [!] Interface de nome

Especifica a interface em que o datagrama foi recebido ou esteja a ser transmitido. Novamente, o `!` inverte o resultado da partida. Se o nome da interface termina com `+`, Então qualquer interface que começa com o apoio da string dobraram irá corresponder. Por exemplo, `-I ppp +` corresponde a nenhum dispositivo de rede PPP e `-I ! eth +` que correspondem a todas as interfaces, exceto os dispositivos Ethernet.

[!]-F

Especifica que esta regra se aplica a tudo, mas o primeiro fragmento de um datagrama fragmentado.

Opções

Os seguintes `ipchains` opções são de natureza mais geral. Alguns deles controlar os recursos e não esotéricos da PI software cadeias:

-B

Faz com que o comando para gerar duas regras. Uma regra coincide com os parâmetros fornecidos, e os outros regra adicionada coincide com os parâmetros correspondentes no sentido inverso.

-V

Causas `ipchains` a ser detalhado na sua saída. Ele irá fornecer mais informações.

-N

Causas `ipchains` para mostrar o endereço IP e portas como números sem tentar resolvê-los para seus nomes correspondentes.

-L

Permite kernel registro de datagramas correspondentes. Qualquer datagrama que coincide com a regra será registrado pelo
o kernel usando o seu *printk ()* função, que normalmente é tratado pelo `sysklogd` programa e escrita em um arquivo de log. Isso é útil para a tomada de datagramas incomum visível.

-O [maxsize]

Faz com que o software IP cadeias de copiar qualquer datagramas correspondente à regra do "netlink" userspace device. O argumento maxsize limita o número de bytes de cada datagrama que são passados para a rede-link dispositivo. Esta opção é mais usado para desenvolvedores de software, mas pode ser explorada por pacote de software
idades no futuro.

M markvalue

Faz com que a correspondência de datagramas *marcada* com um valor. Mark valores não são assinados números de 32 bits. Em ex-
tentes implementações isso não faz nada, mas em algum ponto no futuro, pode determinar como o datagrama é tratado por outros softwares, como o código de roteamento. Se um markvalue começa com uma `+` ou `-`, O valor é adicionado ou subtraído do markvalue existentes.

T xormask andmask

Permite que você manipule o "tipo de serviço" bits no cabeçalho IP de qualquer datagrama que corresponde a esta regra. O tipo de serviço de bits são usados por roteadores inteligentes para priorizar antes de encaminhar datagramas elas. O software de roteamento do Linux é capaz de priorização deste tipo. A *andmask* e *xormask* Represen-enviado máscaras de bits que serão logicamente ANDed e ORed com o tipo de serviço de bits do datagrama re-pectivamente. Este é um recurso avançado que é discutido em detalhes no ipchains-HOWTO.

-X

Faz com que todos os números na `ipchains` saída a ser expandido para seus valores exatos, sem arredondamentos.

-Y

Faz com que a regra para combinar com qualquer datagrama TCP com o bit SYN e ACK e FIN bits claro. Este é usado para filtrar as solicitações de conexão TCP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Nosso exemplo ingênuo Revisited

Vamos novamente supor que temos uma rede em nossa organização e que nós estamos usando um firewall

baseado em Linux
máquina para permitir que nossos usuários acesso a servidores WWW na Internet, mas para permitir que nenhum outro tráfego a serem passados.

Se a nossa rede tem uma máscara de rede de 24 bits (classe C) e tem um endereço de 172.16.1.0, usaríamos o

seguinte
`ipchains` regras:

```
# ipchains-F para a frente
# ipchains-P FORWARD DENY
# ipchains-A FORWARD-s 0 / 0 80-d 172.16.1.0/24-p tcp NEGAR-y-j
# ipchains-A FORWARD-s 172.16.1.0/24-d 0 / 0 80-p tcp ACCEPT-b-j
```

O primeiro dos comandos libera todas as regras da `frente` rulesets eo segundo conjunto de comandos define a política padrão da `frente` conjunto de regras para `NEGAR`. Finalmente, os comandos do terceiro e quarto específico filtragem que queremos. O quarto comando permite datagramas de e para servidores web do lado de fora da nossa rede para passar, eo terceiro impede conexões TCP com uma porta de origem 80.

Se agora queria adicionar regras que permitiu o acesso de modo passivo apenas a servidores de FTP na rede externa, nós adicionar estas regras:

```
# ipchains-A FORWARD-s 0 / 0 20-d 172.16.1.0/24-p tcp NEGAR-y-j
# ipchains-A FORWARD-s 172.16.1.0/24-d 0 / 0 20-p tcp ACCEPT-b-j
# ipchains-A FORWARD-s 0 / 0 21-d 172.16.1.0/24-p tcp NEGAR-y-j
# ipchains-A FORWARD-s 172.16.1.0/24-d 0 / 0 21-p tcp ACCEPT-b-j
```

Listagem de nossas regras ipchains

Para listar as nossas regras com `ipchains`, Usamos os seus *-L* argumento. Assim como ocorre com `ipfwadm`, Há argumentos

que con-
controle a quantidade de detalhes na saída. Na sua forma mais simples, `ipchains` produz um resultado que parece:

```
# ipchains-L-n
Chain INPUT (política ACCEPT):
Chain FORWARD (política de DENY):
alvo       prot opt     fonte               destino             portas
NEGAR      tcp  -----Y  0.0.0.0 / 0         172.16.1.0/24       80 ->   *
ACCEPT     tcp  ------  172.16.1.0/24       0.0.0.0 / 0         * ->   80
ACCEPT     tcp  ------  0.0.0.0 / 0         172.16.1.0/24       80 ->   *
ACCEPT     tcp  ------  172.16.1.0/24       0.0.0.0 / 0         * ->   20
ACCEPT     tcp  ------  0.0.0.0 / 0         172.16.1.0/24       20 ->   *
ACCEPT     tcp  ------  172.16.1.0/24       0.0.0.0 / 0         * ->   21
ACCEPT     tcp  ------  0.0.0.0 / 0         172.16.1.0/24       21 ->   *

Cadeia de saída (política ACCEPT):
```

Se você não fornecer o nome de uma cadeia de lista, `ipchains` irá listar todas as regras em todas as cadeias. A `-N` argumento

em
nosso exemplo, diz `ipchains` não tentar converter qualquer endereço ou portos em nomes. A informação pré-tantes devem ser auto-explicativo.

Uma forma detalhada, invocada pela *-U* opção, oferece muito mais detalhes. Sua saída adiciona campos para o datagrama e contadores de bytes, tipo de serviço *E* e *XOR* bandeiras, o nome da interface, a marca ea desmedida.

Todas as regras criadas com `ipchains` ter datagrama e contadores de bytes associados a eles. Isto é como IP Ac-contagem é implementado e será discutido em detalhes no Capítulo 10. Por padrão, esses contadores são apresentados na uma forma arredondada com os sufixos `K` e `M` para representar unidades de mil e um milhão, respectivamente. Se o `-X` argumento for fornecido, os contadores são expandidos para sua forma plena não arredondados.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Fazendo bom uso das Cadeias

Você já sabe que o `ipchains` comando é um substituto para o `ipfwadm` com uma simples linha de comando sintaxe e algumas melhorias interessantes, mas sem dúvida você está querendo saber onde você pode usar o usuário cadeias definidas e por quê. Você provavelmente também querem saber como usar os scripts de suporte que acompanham o `ipchains` de comando em seu pacote de software. Vamos agora explorar estes assuntos e abordar as questões.

cadeias definidas pelo usuário

Os três conjuntos de regras do código tradicional firewall IP fornecido um mecanismo para a criação de configurações de firewall que foram bastante simples de entender e gerenciar redes de pequeno porte com requisitos simples firewall. Quando os requisitos de configuração não são simples, uma série de problemas se tornam aparentes. Em primeiro lugar, ampla rede de serviços funciona muitas vezes exigem muito mais do que o pequeno número de regras de firewall que vimos até agora; inevitavelmente necessidades surgir que requerem regras de firewall adicionado para cobrir cenários especiais. Como o número de regras cresce, a per- desempenho do firewall deterioriates testes, cada vez mais são realizadas em cada datagrama e gerenciabilidade se torna um problema. Em segundo lugar, não é possível ativar e desativar conjuntos de regras atomicamente, em vez disso, você está forçados a expor-se ao ataque, enquanto você está no meio de reconstruir suas regras.

O projeto do IP Firewall Chains ajuda a aliviar esses problemas, permitindo que o administrador de rede criar conjuntos de regras arbitrárias firwewall que pode ligar para os três conjuntos de regras de inbuilt. Podemos usar o *-N* opção de `ipchains` para criar uma nova cadeia com qualquer nome que quisermos de oito caracteres ou menos. (Restringir o nome para letras minúsculas só é provavelmente uma boa idéia.) A *-J* opção configura a acção a tomar quando um datagrama corresponda às especificações da norma. A *-J* opção especifica que, se um datagrama corresponde a uma regra, mais testes devem ser realizados contra uma chain definida pelo usuário. Vamos ilustrar isto com um diagrama.

Considere o seguinte `ipchains` comandos:

```
ipchains-P input DENY
tcpin ipchains-N
ipchains-A tcpin-s! 172.16.0.0/16
ipchains-A tcpin-p tcp-d 172.16.0.0/16-j ACCEPT ssh
ipchains-A tcpin-p tcp-d 172.16.0.0/16-j ACCEPT www
ipchains-A input-p tcp-j tcpin
ipchains-A input-p todos
```

Vamos definir o padrão de entrada para a política da cadeia `negar`. O segundo comando cria uma chain definida pelo usuário chamada "tcpin".
O terceiro comando adiciona uma regra para o `tcpin` cadeia que combina com qualquer datagrama que foi adquirido de fora nossa rede local, a regra não toma nenhuma providência. Esta regra é uma regra contábil e será discutida mais detalhadamente no Capítulo 10. As próximas duas regras encontraram datagrama que é destinado para a nossa rede local e um dos `ssh` ou `www` portos; datagramas que correspondam a estas regras são aceitas. A próxima regra é quando o real *ipchains* mágica começa.
Isso faz com que o software de firewall para verificar qualquer datagrama do protocolo TCP contra a cadeia tcpin definidos pelo usuário.
Finalmente, nós adicionamos uma regra para o nosso `Entrada` cadeia que combina com qualquer datagrama, esta é uma outra regra contábil. Eles produzir os seguintes correntes Firewall mostrado na Figura 9-4.

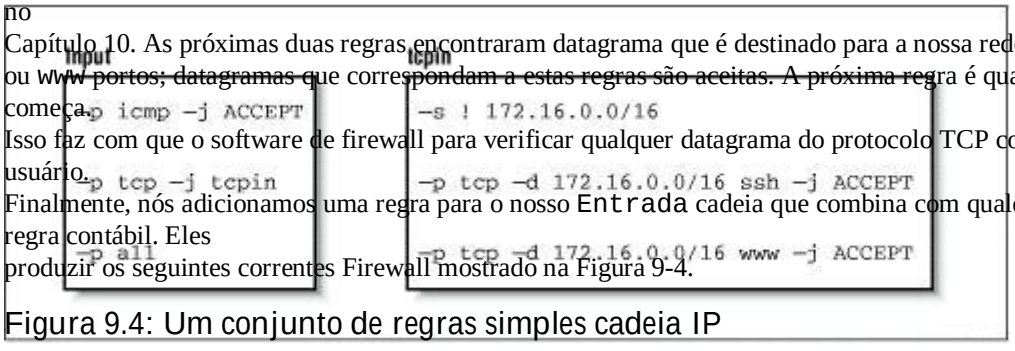


Figura 9.4: Um conjunto de regras simples cadeia IP

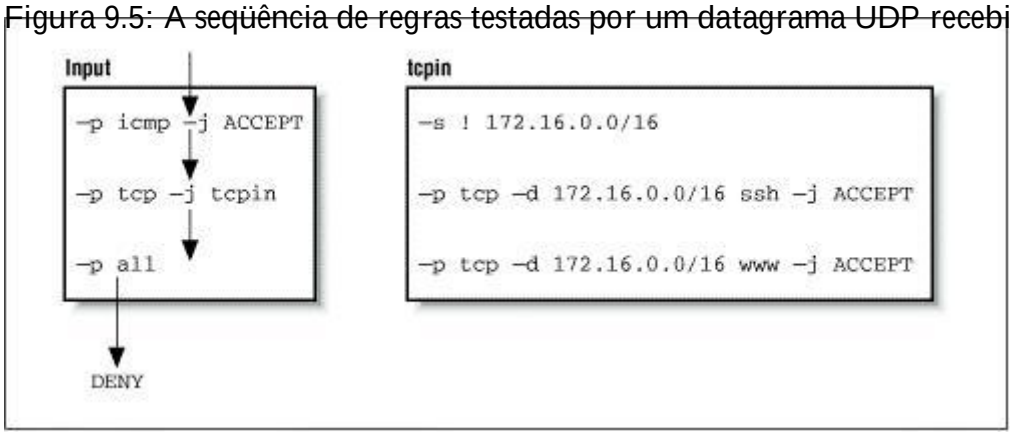
PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Nossa `Entrada` e `tcpin` cadeias são preenchidos com as nossas regras. Datagram processamento sempre seres em um dos Redes de inbuilt. Vamos ver como a nossa cadeia definida pelo usuário é chamado no jogo seguindo o caminho de processamento de dife-
diferentes tipos de datagramas.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Primeiro, vamos olhar o que acontece quando um datagrama UDP para um dos nossos anfitriões é recebida. Figura 9.5 illudemonstra a
fluxo através das regras.

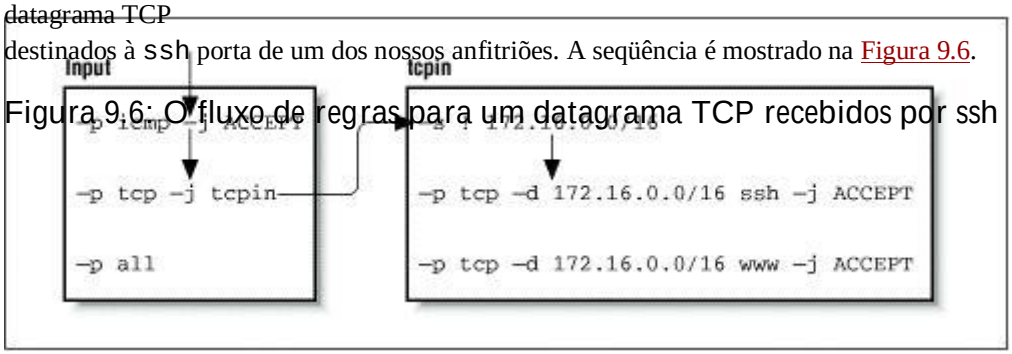
Figura 9.5: A seqüência de regras testadas por um datagrama UDP recebidos



O datagrama é recebido pelo `Entrada` cadeia e cai pelas duas primeiras regras, porque elas correspondem ICMP e protocolos TCP, respectivamente. Ele corresponde a terceira regra na `Entrada` cadeia, mas não especifica um alvo, pelo que a sua
contadores de datagramas e de bytes são atualizados, mas nenhuma outra acção tem lugar. O datagrama chega ao final do `Entrada` cadeia, encontra-se com o padrão `Entrada` política de cadeia, e é negado.

Para ver a nossa cadeia definida pelo usuário em funcionamento, vamos agora considerar o que acontece quando recebemos um datagrama TCP
destinados à `ssh` porta de um dos nossos anfitriões. A seqüência é mostrado na Figura 9.6.

Figura 9.6: O fluxo de regras para um datagrama TCP recebidos por ssh

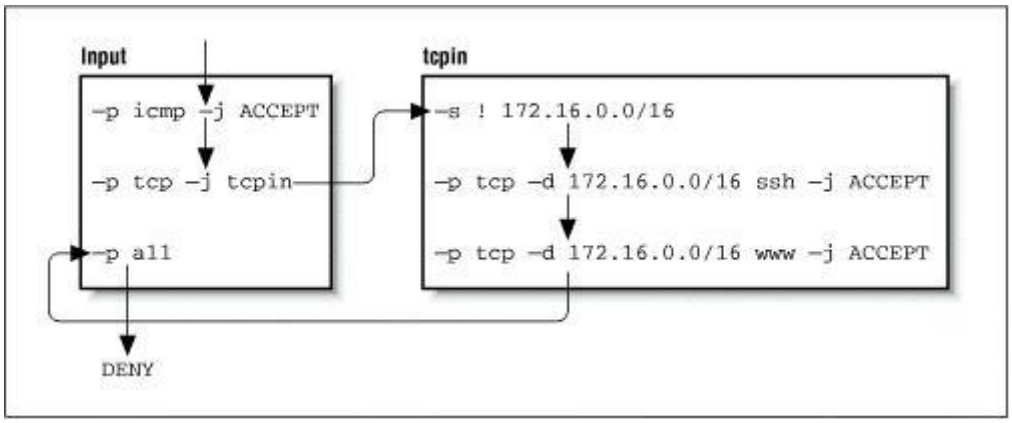


Desta vez, a regra segundo a `Entrada` corrente, fósforo e especifica uma meta de `tcpin`, O nosso definido pelo usuário cadeia. Especificando uma chain definida pelo usuário como um destino faz com que o datagrama a ser testada contra as regras da referida cadeia,
então a próxima regra testada é a primeira regra da `tcpin` cadeia. A primeira regra corresponde a qualquer datagrama que tem uma fonte
endereço fora da nossa rede local e não especifica nenhuma meta, por isso também é uma regra de contabilidade e testes cai através
para a próxima regra. A segunda regra em nosso `tcpin` corrente, fósforo e especifica uma meta de ACCEPT. Temos chegou ao destino, portanto, nenhum processamento firewall ainda ocorre. O datagrama é aceito.

Finalmente, vamos ver o que acontece quando chegamos ao fim de uma chain definida pelo usuário. Para ver isso, vamos mapear o fluxo de
para um datagrama TCP com destino a uma porta diferente da que os dois estamos a tratar especificamente, como mostrado na Figura
9.7.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Figura 9.7: O fluxo de regras para um datagrama TCP recebidos de telnet



As cadeias definidas pelo usuário não tem políticas padrão. Quando todas as regras de uma chain definida pelo usuário foram testados,
e ninguém tem correspondido, o código de firewall funciona como se uma `RETORNO` Estado estavam presentes, então, se este não é o que você
quer, você deve se assegurar que você fornecer uma regra no fim da chain definida pelo usuário que tenha qualquer ação que você
desejo. No nosso exemplo, nossos retornos de testes para a regra no `Entrada` ruleset imediatamente após o que
nos levou ao nosso chain definida pelo usuário. Finalmente, chegamos ao final do `Entrada` cadeia, que tem um padrão política e os nossos datagrama é negado.

Este exemplo é muito simples, mas ilustra o nosso ponto. Um uso mais prático das cadeias de IP seria muito mais complexo. Um exemplo um pouco mais sofisticado é fornecida na seguinte lista de comandos:

```
#
# Definir a política de encaminhamento padrão para REJEITAR
ipchains-P frente REJEITAR
#
# Criar nossas cadeias definidas pelo usuário
sshin ipchains-N
sshout ipchains-N
wwwin ipchains-N
wwwout ipchains-N
#
# Certifique-se rejeitar conexões vindo na direção errada
172.16.0.0/16 ipchains-A wwwin-p tcp-s-y-j REJECT
ipchains-A wwwout-p tcp-d 172.16.0.0/16 REJECT-y-j
172.16.0.0/16 ipchains-A sshin-p tcp-s-y-j REJECT
ipchains-A sshout-p tcp-d 172.16.0.0/16 REJECT-y-j
#
# Certifique-se que nada de chegar ao fim de uma chain definida pelo usuário é re-
projetada.
ipchains-rejeitar uma sshin-j
ipchains-rejeitar uma sshout-j
ipchains-rejeitar uma wwwin-j
ipchains-rejeitar uma wwwout-j
#
# Desviar serviços www e ssh para a cadeia relevantes definidos pelo usuário
ipchains-A FORWARD-p tcp-d 172.16.0.0/16 sshin ssh-b-j
ipchains-A FORWARD-p tcp-s 172.16.0.0/16-d 0 / 0 sshout ssh-b-j
ipchains-A FORWARD-p tcp-d 172.16.0.0/16 wwwin www-b-j
ipchains-A FORWARD-p tcp-s 172.16.0.0/16-d 0 / 0 wwwout www-b-j
#
# Inserir as nossas regras para combinar hospeda na posição dois, no nosso definido
pelo usuário
cadeias.
ipchains-I wwwin ACEITA 2-d 172.16.1.2-b-j
ipchains-I wwwout 2 s-ACCEPT 172.16.1.0/24-b-j
ipchains-I sshin ACEITA 2-d 172.16.1.4-b-j
ipchains-I sshout 2 s-ACCEPT 172.16.1.4-b-j
ipchains-I sshout 2 s-ACCEPT 172.16.1.6-b-j
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

#

Neste exemplo, usamos uma seleção de cadeias definidas pelo usuário, tanto para simplificar o gerenciamento de firewall nosso con-
figuração e melhorar a eficiência de nosso firewall, em comparação com uma solução envolvendo apenas as chains.

Nosso exemplo cria cadeias definidas pelo usuário para cada um dos `ssh` e `www` serviços em cada sentido da conexão. A corrente chamada `wwwout` é onde colocar as regras para os hosts que estão autorizados a saída da World Wide Web conexões, e `sshin` é onde se define as regras para os anfitriões aos quais deseja permitir conexões de ssh.
Nós supor que nós temos a obrigação de permitir e negar hosts individuais em nossa rede a capacidade de fazer ou receber `ssh` e `www` conexões. O Simplicação ocorre porque as cadeias definidas pelo usuário permitem ordenadamente o grupo de regras para as permissões de entrada e saída de acolhimento, em vez de confundi-los todos juntos.
O aumento da eficiência ocorre porque para qualquer datagrama particular, nós reduzimos o número médio dos testes necessários antes de um alvo é encontrado. O ganho aumenta a eficiência à medida que adicionar mais hosts. Se não tivéssemos usado
chains definidas pelo usuário, nós temos potencial para pesquisar toda a lista de regras para determinar quais as medidas a tomar com
cada um e cada datagrama recebido. Mesmo se assumirmos que cada uma das regras em nossa lista corresponde a uma proporção igual-
ção do número total de datagramas processado, ainda estaríamos procurando metade da lista, em média. Definidos pelo usuário correntes nos permitem evitar testes um grande número de regras, se o datagrama está sendo testado não corresponde à simples regra
na built-in em cadeia que vai para eles.

O ipchains scripts de suporte

A `ipchains` pacote de software é fornecido com três roteiros de apoio. A primeira delas nós já discutimos já brevemente, enquanto os dois restantes oferecem um meio fácil e conveniente de salvar e restaurar a sua configuração do firewall.

A `ipfwadm-wrapper` script emula a sintaxe de linha de comando do `ipfwadm` comando, mas conduz o `ipchains` comando para criar regras de firewall. Esta é uma maneira conveniente para migrar o firewall existente configuração para o kernel ou uma alternativa à aprendizagem da `ipchains` sintaxe. A `ipfwadm-wrapper` script se comporta de forma diferente da `ipfwadm` comando de duas maneiras: primeiro, porque a `ipchains` comando faz-especificação apoio n't de uma interface de endereço, o `ipfwadm-wrapper` script aceita um argumento de *-V* mas tenta convertê-lo para o `ipchains` equivalente a um *-W* pesquisando o nome da interface configurada com o endereço fornecido. A `ipfwadm-wrapper` script será sempre um aviso quando você usa o *-V* opção para lembrá-lo disso. Em segundo lugar, as regras contabilísticas fragmento não são traduzidos corretamente.

A `ipchains-save` e `ipchains-restore` scripts tornam a construção e modificação de uma configuração de firewall ção muito mais simples. A `ipchains-save` comando lê a configuração do firewall e escreve um sim-
plified formulário para a saída padrão. A `ipchains-restore` comando lê os dados no formato de saída do `ipchains-save` comando e configura o firewall IP com estas regras. A vantagem do uso dessas scripts mais diretamente modificar o script de configuração do firewall e testar a configuração é a capacidade de construir dinamicamente a configuração de uma vez e depois salvá-lo. Você pode restaurar essa configuração, modificá-lo e salve-a como quiser.

Para usar os scripts, você pode digitar algo como:

```
ipchains-save> / var / state / ipchains / firewall.state
```

para salvar sua configuração do firewall. Você restaurá-lo, talvez em tempo de boot, com:

```
ipchains-restore </ var / state / ipchains / firewall.state
```

A `ipchains-restore` script verifica se algum chain definida pelo usuário listado em sua entrada já existe. Se você forneceu a `-F` argumento, ele será automaticamente liberado das regras da chain definida pelo usuário antes de configurar os na entrada. O comportamento padrão pergunta-lhe se para saltar esta cadeia ou para nivelá-lo.

Netfilter e iptables (kernel 2.4)

Durante o desenvolvimento do firewall IP Chains, Paul Russell decidiu que o firewall IP deve ser menos difícil, ele logo conjunto sobre a tarefa de simplificar os aspectos do processamento de datagramas no código do kernel do firewall e produziu um
filtragem de quadro que foi ao mesmo tempo muito mais limpo e muito mais flexível. Ele chamou este novo quadro *netfilter*.

Observação: No momento da elaboração deste livro *netfilter* projeto ainda não havia estabilizado. Esperamos que te perdoe algum erro na descrição do *netfilter* ou das suas ferramentas de configuração, assumindo que não tenham de mudanças que ocor-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

reu após a preparação deste material. Foi considerado o *netfilter* trabalho importante suficiente para justificar a inclu-
Sion deste material, apesar de partes de ser de natureza especulativa. Se você estiver em dúvida, o HOWTO relevante

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

documentos deverão conter as informações mais precisas e atualizadas sobre as questões associadas à execução *netfilter* configuração.

Então, o que havia de errado com cadeias IP? Eles melhoraram muito a eficiência ea gestão de regras de firewall. Mas a maneira como eles processados datagramas ainda era complexa, especialmente em conjunto com recursos de firewall-relacionados como IP mascarado (discutido no Capítulo 11) e outras formas de tradução de endereços. Parte desta complexidade existiu porque o IP mascarado e Network Address Translation foram desenvolvidos independentemente do IP firewall código e integrado mais tarde, ao invés de ter sido concebido como uma parte verdadeira do código de firewall desde o início. Se um desenvolvedor queria acrescentar características ainda mais na seqüência de processamento de datagramas, ele teria dificuldade encontrar um lugar para inserir o código e que teria sido forçado a fazer alterações no kernel, a fim de fazê-lo.

Ainda assim, houve outros problemas. Em particular, o "input" cadeia descrito entrada para a camada de rede IP como um inteiro. A cadeia de insumos afetou tanto datagramas para ser *destinados a* este acolhimento e datagramas para ser *encaminhado pelo* presente host. Este foi um tanto esquisito, pois confundiu a função da cadeia de entrada com o da cadeia para frente, o que apenas se aplicava aos datagramas para ser transmitida, mas que sempre seguiu a corrente de entrada. Se você quis tratar datagramas para este host diferente de datagramas para ser encaminhado, foi necessário construir regras complexas que uma exclusão ou a outra. O mesmo problema aplicado à cadeia de produção.

Inevitavelmente, alguns desta complexidade transbordou para o trabalho do administrador do sistema, porque se refletiu na maneira que rulesets teve de ser concebido. Além disso, todas as extensões de filtragem necessária modificações directo à kernel, porque todas as políticas de filtragem foram implementadas lá e não havia maneira de proporcionar uma forma transparente interface para ele. *netfilter* aborda tanto a complexidade ea rigidez das velhas soluções através da implementação de um estrutura genérica no kernel que simplifica a forma de datagramas são processados e fornece uma capacidade de estender a filtragem política sem ter que modificar o kernel.

Vamos dar uma olhada em duas das principais mudanças feitas. Figura 9.8 illudemonstra como os datagramas são processados no PI cadeias de execução, enquanto Figura 9.9 illudemonstra como eles são tratados no *netfilter* implementação. A principais diferenças são a remoção da função de mascaramento do código do núcleo e uma mudança nos locais de as correntes de entrada e saída. Para acompanhar essas mudanças, uma nova ferramenta de configuração e extensível chamada `IPT-veis` foi criado.

Nas cadeias de IP, a cadeia de entrada se aplica a todos os datagramas recebidos pelo anfitrião, independentemente de se tratar de destined para o host local ou encaminhados para algum outro host. Em *netfilter*, A cadeia de entrada se aplica *apenas* datagramas destined para o host local, e da cadeia para a frente só se aplica aos datagramas destinados a *outro* host. Da mesma forma, em Redes IP, a cadeia de produção se aplica a todos os datagramas deixando a máquina local, independentemente de o datagrama é gerada na máquina local ou encaminhados de algum outro host. Em *netfilter*, A corrente de saída se aplica *apenas* de dados gramas produzidos nessa máquina e não se aplica aos datagramas ser encaminhados a partir de outro host. Essa mudança só oferece uma enorme simplificação das configurações de firewall muitos.

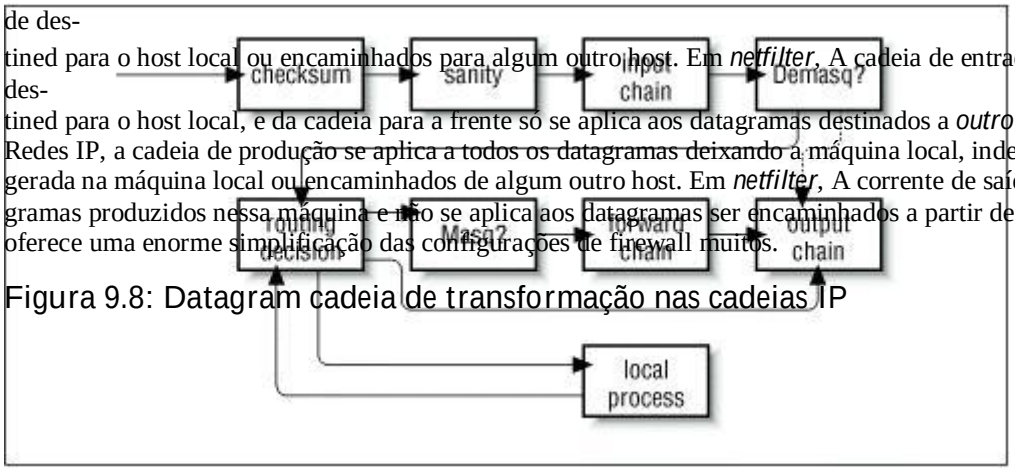


Figura 9.8: Datagram cadeia de transformação nas cadeias IP

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Em Figura 9.8,os componentes do chamado "demasq" e "máscara" são componentes do kernel separados responsável pela processamento de entrada e saída de datagramas mascarados. Estes têm sido reimplantado como *netfilter* mod-REGRAS.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Considere o caso de uma configuração para que a política padrão para cada uma das entradas, para a frente,

ea saída
cadeias é `negar`. Nas cadeias de IP, seis regras seriam necessárias para permitir que qualquer sessão através de um firewall de host: dois em cada
a entrada, em frente, correntes e de saída (seria cobrir cada caminho para a frente e iria cobrir cada caminho de ida e volta). Você pode imaginar como isso poderia facilmente tornar-se extremamente complexa e difícil de gerir quando você quiser sessões de mistura que pode ser roteado e sessões que podem se conectar ao host local sem ser roteado. IP
Redes permitem que você crie cadeias que simplificar esta tarefa um pouco, mas o projeto não é óbvia e exige uma certo nível de especialização.

Na *netfilter* execução, com `iptables`, Esta complexidade, desaparece completamente. Para um serviço a ser encaminhado através do firewall de host, mas não terminar no host local, apenas duas regras são necessárias: uma para cada uma das
frente e verso as instruções na cadeia para a frente. Esta é a maneira mais óbvia de criar regras de firewall, e servirá para simplificar o projeto de configurações de firewall imensamente.

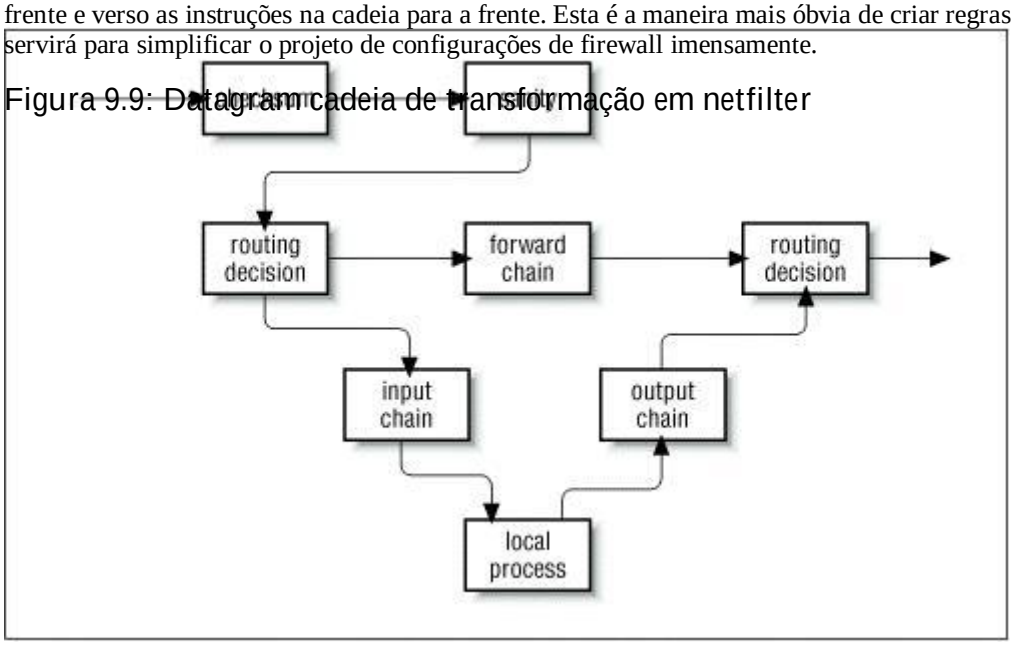


Figura 9.9: Datagram cadeia de transformação em netfilter

A filtragem de pacotes-HOWTO oferece uma lista detalhada das alterações que foram feitas, por isso vamos nos concentrar na os aspectos mais práticos aqui.

Compatibilidade com versões anteriores com ipfwadm e ipchains

A notável flexibilidade do Linux *netfilter* é ilustrada pela sua capacidade de imitar o `ipfwadm` e `ipchains` interfaces. Emulação faz a transição para a nova geração de software de firewall um pouco mais fácil.

Os dois *netfilter* módulos do kernel chamada *ipfwadm.o* e *ipchains.o* fornecer compatibilidade com versões anteriores para

`ipfwadm`
e `ipchains`. Você pode carregar apenas um desses módulos em um momento, e usar um apenas se o *ip_tables.o* módulo não está carregado. Quando o módulo apropriado é carregado, *netfilter* funciona exatamente como a aplicação de firewall ex-ção.

netfilter imita o `ipchains` interface com os seguintes comandos:

```
ip_tables rmmod
modprobe ipchains
ipchains ...
```

Usando o iptables

A `iptables` utilitário é usado para configurar *netfilter* regras de filtragem. Sua sintaxe se baseia fortemente na `ip-`

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`cadeias` comando, mas difere em um aspecto muito importante: é *extensível*. O que isto significa é que a sua fun-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

nalidade pode ser estendido sem recompilá-lo. Ele gerencia este truque usando bibliotecas compartilhadas. Há nor-
Extensões padrão e vamos explorar alguns deles em um momento.

Antes que você possa usar o `iptables` comando, você deve carregar o *netfilter* módulo do kernel que fornece suporte
para isso. A maneira mais fácil de fazer isso é usar o `modprobe` comando da seguinte forma:

```
ip_tables modprobe
```

A `iptables` comando é usado para configurar o IP de filtragem e Network Address Translation. Para facilitar
isso, existem duas mesas de regras denominado *filtro* e *nat*. A tabela filter é assumido se você não especificar o *T*
opção para substituí-lo. Cinco chains são também fornecidos. A `INPUT` e `EXPECTATIVA` cadeias estão disponíveis para
o `filtro` tabela, o `PREROUTING` e `POSTROUTING` cadeias estão disponíveis para o `nat` mesa, e os `FORA`
`PUT` cadeia está disponível para ambas as tabelas. Neste capítulo, vamos discutir apenas o *filtro* tabela. Vamos olhar para o *nat* tabela
no capítulo 11

A sintaxe mais geral `iptables` comandos é:

`iptables` *comando extensões especificação de regras*

Agora vamos dar uma olhada em algumas opções em detalhe, após o qual vamos analisar alguns exemplos.

Comandos

Há uma série de maneiras que podemos manipular as regras e conjuntos de regras com o `iptables` comando. Aqueles

relevantes
para o firewall IP são:

-A cadeia

Acrescente uma ou mais regras para a final da cadeia de nomeada. Se um nome de host é fornecido tanto como uma
fonte
ou de destino e ele resolve para mais de um endereço IP, uma regra será adicionada para cada endereço.

-I cadeia rulenum

Insira uma ou mais regras para o início da cadeia de nomeada. Novamente, se uma máquina é fornecida na regra especificação, uma regra será adicionada para cada um dos endereços para os quais ele resolve.

-D cadeia

Excluir uma ou mais regras da cadeia especificada acordo com a especificação de regras.

-D chain rulenum

Eliminar a regra que residem na posição *rulenum* na cadeia especificada. Regra posições começam em 1 para o
primeiro
regra da cadeia.

-R chain rulenum

Substituir a regra que residem na posição *rulenum* na cadeia específica com a especificação fornecida regra.

-C cadeia

Verifique o datagrama descrito pela especificação regra contra a corrente específica. Este comando
retornar uma mensagem descrevendo como a cadeia processou o datagrama. Isto é muito útil para testar o seu
configuração de firewall e veremos em detalhe mais tarde.

-L [cadeia]

Listar as regras da cadeia especificada, ou para todas as cadeias se nenhuma corrente é especificada.

-F [chain]

Lave as regras da cadeia especificada, ou para todas as cadeias se nenhuma corrente é especificada.

-Z [cadeia]

Zerar os contadores de datagramas e de bytes para todas as regras da cadeia especificada, ou para todas as cadeias se
nenhuma corrente é
especificado.

-N cadeia

Criar uma nova cadeia com o nome especificado. Uma cadeia de mesmo nome, não deve existir. Esta é

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

como cadeias definidas pelo usuário são criados.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

-X [cadeia]

Eliminar a cadeia definido pelo usuário, ou todas as chains definidas pelo usuário se não houver

corrente é especificada. Para este
comando para ser bem sucedido, não deve haver referências à cadeia especificada de quaisquer outras regras
cadeia.

-P cadeia política

Definir a política padrão da cadeia especificada para a política especificada. as políticas de firewall são válidos `ACCEPT`,`DROP`,`FILA`E `RETORNO`.`ACCEPT` permite que o datagrama passar. `DROP` faz com que o datagrama
ser descartados. `FILA` faz com que o datagrama a ser passado ao userspace para processamento adicional. A `REVOLTA` destino faz com que o código do IP firewall para retornar à Cadeia Firewall que chamou a um contendo
esta regra, e continuar iniciando na regra após a regra de chamada.

especificação de parâmetros da regra

Há uma série de `iptables` parâmetros que constituem uma especificação da regra. Sempre que uma norma de especificação
É necessário, cada um destes parâmetros devem ser entregues ou seu padrão será adotado.

-P [!] Protocolo

Especifica o protocolo de datagrama que irá corresponder a essa regra. nomes de protocolos válidos são `tcp`,`udp`, `icmp`, Ou um número, se você souber o número do protocolo IP.[64] Por exemplo, você pode usar `4` para coincidir com o `ipip` encapsulamento protocolo. Se o `!` personagem é fornecida, a regra é negada eo datagrama será
corresponder a qualquer outro protocolo que o protocolo especificado. Se este parâmetro não for fornecido, o padrão será
corresponder a todos os protocolos.

-S [!] Endereço [/ mask]

Especifica o endereço de origem do datagrama que irá corresponder a essa regra. O endereço pode ser fornecido como

um
hostname, nome de uma rede ou um endereço IP. O opcional `máscara` é a máscara para usar e pode ser sup-
dobrado na forma tradicional (por exemplo, / 255.255.255.0) ou sob a forma moderna (por exemplo, / 24).

-D [!] Endereço [/ mask]

Especifica o endereço de destino ea porta do datagrama que irá corresponder a essa regra. A codificação deste parâmetro é a mesma que a do *-S* parâmetro.

J-alvo

Especifica que ação tomar quando esta regra encontrados. Você pode pensar desse parâmetro no sentido de "salto para. metas "válidos são `ACCEPT`,`DROP`,`FILA`E `RETORNO`. Descrevemos os significados de cada uma das
estes previamente no "Comandos" seção. Você também pode especificar o nome de uma chain definida pelo usuário quando o tratamento vai continuar. Você também pode fornecer o nome de um objectivo fornecido por uma extensão. Vamos falar sobre as extensões em breve. Se este parâmetro for omitido, nenhuma ação será tomada sobre a adequação de dados
gramas em tudo, além de atualizar os contadores de datagramas e de bytes de esta regra.

-I [!] Interface de nome

Especifica a interface em que o datagrama foi recebido. Novamente, o `!` inverte o resultado da partida.
Se o nome da interface termina com "+"Então, qualquer relação que começa com a seqüência fornecida irá corresponder.
Por exemplo, `-I ppp +` corresponde a nenhum dispositivo de rede PPP e `-I! eth +` iria corresponder a todos os inter-
faces, exceto dispositivos de rede.

-O [!] Interface de nome

Especifica a interface na qual o datagrama deve ser transmitida. Este argumento tem a mesma codificação como o *-I* argumento.

[!]-F

Especifica que esta regra se aplica apenas ao segundo fragmento e depois de um datagrama fragmentado, não o primeiro fragmento.

Opções

Os seguintes `iptables` opções são de natureza mais geral. Alguns deles controlar os recursos e não esotéricos da

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

o *netfilter* software.

64 Dê uma olhada */ Etc / protocols* para nomes e números de protocolo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

-V

causas `iptables` a ser detalhado em sua saída, que irá fornecer mais informações.

-N

causas `iptables` para mostrar o endereço IP e portas como números sem tentar resolvê-los para seus nomes correspondentes.

-X

faz com que todos os números na `iptables` saída a ser expandido para seus valores exatos, sem arredondamentos.

--Line-numbers

faz com que os números de linha a ser exibido quando rulesets anúncio. O número da linha corresponderá ao da regra posição dentro da cadeia.

Extensões

Dissemos anteriormente que o `iptables` utilitário é extensível através de módulos opcionais de biblioteca compartilhada. Há alguns
extensões padrão que fornecem algumas das funcionalidades `ipchains` fornecidas. Para fazer uso de uma extensão, que deve especificar seu nome através do *M nome* argumento para `iptables`. A lista a seguir mostra o *M* e *-P* opções que configuram o contexto de extensão, e as opções oferecidas por essa extensão.

Extensões TCP: usado com p tcp-m tcp-

- O desporto [[porta: porta]] [!]

Especifica a porta que a origem do datagrama deve estar usando para coincidir com esta regra. As portas podem ser especificadas como um
escala, especificando o limite superior e inferior do intervalo com os dois pontos como um delimitador. Por exemplo, `20:25` descritas todas as portas numeradas de 20 até e incluindo 25. Novamente, o `!` personagem pode ser utilizado para negar os valores.

- Dport [[port: port]] [!]

Especifica a porta que o destino do datagrama deve estar usando para coincidir com esta regra. O argumento é codificado
de forma idêntica ao *--Esporte* opção.

--Tcp-flags comp máscara [!]

Especifica que esta regra deve corresponder quando as bandeiras TCP no datagrama corresponder aos especificados pelo *máscara*
e *comp.máscara* é uma lista separada por vírgulas de bandeiras que devem ser examinadas ao fazer o teste. *comp* é uma lista separada por vírgulas das bandeiras que devem ser definidas para a regra para combinar. sinalizadores válidos são: *SYN*,*ACK*,*FIN*,
RST,*URG*,*PSH*,*ALL* ou *NONE*. Esta é uma opção avançada: referem-se a uma boa descrição do TCP protocolo, como RFC-793, para uma descrição do significado e implicações de cada uma dessas bandeiras. A `!` personagem atenta contra o Estado.

[!] - Syn-

Especifica a regra para combinar datagramas apenas com o `SYN` conjunto de bits e `ACK` e `FIN` bits limpos. Datagramas com essas opções são usadas para abrir as conexões TCP, e esta opção pode ser usada para gerenciar solicitações de conexão. Esta opção é um atalho para:

```
--Tcp-flags SYN, RST, ACK SYN
```

Quando você usa o operador de negação, o Estado irá corresponder a todos os datagramas que não têm tanto a `SYN` e `ACK` conjunto de bits.

Extensões UDP: usado com p udp-m udp-

- O desporto [[porta: porta]] [!]

Especifica a porta que a origem do datagrama deve estar usando para coincidir com esta regra. As portas podem ser especificadas como um
escala, especificando o limite superior e inferior do intervalo com os dois pontos como um delimitador. Por exemplo, `20:25` descreve todas as portas numeradas de 20 até e incluindo 25. Novamente, o `!` personagem pode ser utilizado para negar os valores.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

- Dport [[port: port]] [!]

Especifica a porta que o destino do datagrama deve estar usando para coincidir com esta regra. O argumento é codificado
de forma idêntica ao *--Esporte* opção.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Extensões ICMP: usado com P icmp-m icmp-

-Icmp-type typename - [!]

Especifica o tipo de mensagem ICMP que a regra irá corresponder. O tipo pode ser especificado em número ou em
nome. Alguns nomes válidos são: `echo-request`,`resposta de eco-`,`source-quench`,`tempo excedido`,`destino inalcançável`,`rede inacessível`,`host-unreachable`, `protocolo inalcançável`E `port-unreachable`.

Extensões MAC: usado com -M mac

- Mac-source-address [!]

Especifica o endereço Ethernet do host que transmitiu o datagrama que esta regra vai corresponder. Isso só faz sentido em uma regra da cadeia de entrada ou para a frente porque nós estaremos transmitindo qualquer datagrama que
passa a corrente de saída.

Nosso exemplo ingênuo Revisited, mais uma vez

Para implementar o nosso exemplo ingênuo usando o *netfilter*, Você pode simplesmente carregar o *ipchains.o* módulo e fingir que é o `ipchains` versão. Em vez disso, vamos reimplementar-lo usando `iptables` para ilustrar como ele é similar.

Mais uma vez, vamos supor que temos uma rede em nossa organização e que nós estamos usando um firewall baseado em Linux máquina para permitir que nossos usuários possam acessar os servidores WWW na Internet, mas para permitir que nenhum outro tráfego a ser
passado.

Se a nossa rede tem uma máscara de rede de 24 bits (classe C) e tem um endereço de 172.16.1.0, então usaríamos o seguinte `iptables` regras:

```
# ip_tables modprobe
# iptables-F FORWARD
# iptables-P FORWARD DROP
# iptables-A FORWARD-p tcp-m tcp-s 0 / 0 - sport 80-d 172.16.1.0/24 /
    - Syn-j DROP
# iptables-A FORWARD-m tcp-p tcp-s 172.16.1.0/24 - esporte /
    80-d 0 / 0-j ACCEPT
# iptables-A FORWARD-m tcp-p tcp-d 172.16.1.0/24 - dport 80-s 0 / 0-j /
    ACCEPT
```

Neste exemplo, o `iptables` comandos são interpretados exatamente como o equivalente `ipchains` comandos. A exceção importante que o *ip_tables.o* módulo deve carregar. Note-se que `iptables` não suporta a *-B* opção, então devemos fornecer uma regra para cada direção.

TOS manipulação de bits

O Type Of Service (TOS) bits são um conjunto de sinalizadores de quatro bits no cabeçalho IP. Quando qualquer um desses sinalizadores é pouco definido,
roteadores podem manipular o datagrama diferente datagramas sem bits TOS set. Cada um dos quatro bits tem um finalidade diferente e apenas um dos bits TOS pode ser fixado a qualquer momento, assim que as combinações não são permitidas. O bit
bandeiras são chamados de bits Tipo de serviço porque permitem a aplicação de transmitir os dados para contar a rede o tipo de serviço de rede que requer.

As classes de serviço de rede disponíveis são:

Retardo mínimo

Usado quando o tempo que leva para um datagrama para viajar a partir do host de origem para destino de acolhimento (latência) é
mais importante. Um provedor de rede pode, por exemplo, usar a fibra óptica e rede de satélites

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

conexões. De dados realizada através de conexões via satélite tem mais para viajar e sua latência geralmente é portanto, superior para conexões de rede terrestre baseado entre os mesmos parâmetros. Uma rede fornecedor pode optar por garantir que os datagramas com este tipo de conjunto de serviços não sejam realizadas por satélite.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A vazão máxima

Usado quando o volume de dados transmitidos em qualquer período de tempo é importante. Existem muitos tipos de aplicativos de rede para que a latência não é particularmente importante, mas o débito da rede é, por exemplo, transferências de arquivos em massa. Um provedor de rede pode optar por encaminhar datagramas com este tipo de servi-
vice-definidas através de alta latência, vias de alta largura de banda, tais como conexões via satélite.

Máxima fiabilidade

Usado quando é importante que você tenha alguma certeza que os dados cheguem ao destino com-
a retransmissão se necessário. O protocolo IP pode ser transportada sobre qualquer número de subjacentes meios de transmissão. Enquanto SLIP e PPP são protocolos de enlace de dados adequada, eles não são tão fiáveis como realização IP sobre alguma outra rede, como uma rede X.25. Um provedor de rede pode fazer uma al-
rede ternate disponíveis, oferecendo alta confiabilidade, para exercer IP que seria usado se este tipo de serviço é selecionado.

custo mínimo

Utilizado quando é importante minimizar o custo de transmissão de dados. Leasing largura de banda de um satélite para uma travessia transpacífica é geralmente menos caro do que aluguel de espaço em um cabo de fibra óptica ao longo dos
mesma distância, para que os provedores de rede podem optar por oferecer tanto e cobrar preços diferentes, dependendo que você usa. Neste cenário, o "custo mínimo" tipo de serviço pouco pode fazer com que seu datagramas ser encaminhado por via satélite de baixo custo.

Definir o TOS ipfwadm Bits Usar ou ipchains

A `ipfwadm` e `ipchains` comandos de acordo com os bits TOS em muito da mesma maneira. Em ambos os casos especificar uma regra que corresponda ao datagramas com particular bits TOS conjunto e usar o *T* argumento para especificar o mudança que você deseja fazer.

As mudanças são especificados usando máscaras de dois bits. A primeira dessas máscaras de bits é logicamente ANDed com a

op-IP
ções de campo do datagrama eo segundo é logicamente exclusivo Ord com ele. Se isso soa complicado, vamos dar-lhe as receitas necessárias para permitir a cada um dos tipos de serviços em um momento.

As máscaras de bits são especificados usando os valores hexadecimal de oito bits. Ambos `ipfwadm` e `ipchains` usar o

mesmo
sintaxe de argumento:

`T` *xormask andmask*

Felizmente, os argumentos mesma máscara pode ser usada cada vez que você deseja definir um tipo específico de serviço, para que não tenha de trabalhar para fora. Eles são apresentados com alguns usos sugeridos no Tabela 9.3.

Tabela 9.3: Usos sugeridos para Bitmask TOS

TOS	ANDmask	XORmask	Sugestão de Uso
Mínimo Atraso	`0x01`	`0x10`	ftp, telnet, ssh
Maximum Throughput	`0x01`	`0x08`	ftp-data, www
Máxima Confiabilidade	`0x01`	`0x04`	SNMP, DNS
Custo Mínimo	`0x01`	`0x02`	NNTP, SMTP

Estabelecer os bits TOS Usando o iptables

A `iptables` ferramenta permite que você especifique as regras que a captura de datagramas apenas com bits TOS

correspondentes a alguns pré-
determinado valor usando o *tos-m* opção, e para a fixação dos bits TOS de datagramas IP que combinam com uma regra usando o

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`TOS-j` alvo. Você pode definir os bits TOS somente no `EXPECTATIVA` e `SAÍDA` cadeias. O casamento ea criação ocorrer de forma totalmente independente. Você pode configurar todo o tipo de regras interessantes. Por exemplo, você pode configurar uma regra
discads que todos os datagramas com combinações de bits TOS, ou uma regra que define os bits TOS de datagramas apenas a partir de certos hosts. Na maioria das vezes você irá usar as regras que contêm correspondência e definição para bit TOS traduções, assim como você poderia, por `ipfwadm` ou `ipchains`.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Mais do que a configuração de duas máscara complicada `ipfwadm` e `ipchains`,`iptables` usa o simples abordagem de especificar claramente o que os bits TOS deve corresponder, ou até que os bits TOS deve ser definido. Adição- aliado, ao invés de ter que se lembrar e usar o valor hexadecimal, você pode especificar os bits TOS usando o mnemônicos mais amigável listados na tabela seguinte.

A sintaxe geral usada para corresponder bits TOS aparência:

`M-tos - TOS` *mnemônico* `[`*outros-args*`]-J` *alvo*

A sintaxe geral usada para definir bits TOS aparência:

`[`*outros-args*`TOS]-j - set` *mnemônico*

Lembre-se que estes seriam normalmente utilizados em conjunto, mas pode ser usado de forma totalmente independente se você tiver um
configuração que requer.

Mnemônico	Hexadecimal
Normal-Service	0x00
Minimizar o custo	0x02
Maximizar a confiabilidade,	0x04
Maximize-Throughput	0x08
Minimize-Delay	0x10

Testando a configuração de um Firewall

Depois de ter desenhado uma configuração de firewall apropriadas, é importante para validar o que ele faz, de facto, fazer o que você quer que ele faça. Uma maneira de fazer isso é usar uma máquina de ensaio fora da sua rede para tentar furar o seu firewall: isto pode ser muito desastrado e lento, porém, e está limitado a testar apenas os endereços que você pode realmente uso.

Um método mais rápido e fácil está disponível com a implementação de firewall Linux. Ele permite que você manualmente geral-
comeu testes e executá-los através da configuração de firewall como se você estivesse testando com datagramas real. Todos variedades do software de firewall do kernel Linux, `ipfwadm`,`ipchains`E `iptables`, Fornecer suporte para esta estilo de teste. A implementação envolve o uso do relevante *seleção* comando.

O procedimento de ensaio geral é o seguinte:

1. Projetar e configurar o firewall utilizando `ipfwadm`,`ipchains`Ou `iptables`.
2. Design de uma série de testes que irá determinar se o firewall está realmente funcionando como você pretende. Para estes testes você pode usar qualquer endereço de origem ou de destino, para escolher algumas combinações de endereços que
devem ser aceitos e alguns outros que devem ser descartados. Se você está permitindo ou não permitindo apenas cer- cordilheiras de endereços, é uma boa idéia testar os endereços de ambos os lados da fronteira da faixa - apenas um endereço dentro da fronteira e um endereço fora do limite. Isto ajudará a assegurar
que você tenha configurado os limites corretos, pois às vezes é fácil especificar máscaras em
corretamente em sua configuração. Se você está filtrando por número de protocolo e porta, os testes também devem checar todas as combinações importantes destes parâmetros. Por exemplo, se você pretende aceitar apenas TCP em certas circunstâncias, verificar que os datagramas UDP são descartados.
3. Desenvolver `ipfwadm`,`ipchains`Ou `iptables` normas de execução de cada teste. É provavelmente vale a pena para escrever todas as regras em um script para que você possa testar e re-teste facilmente como você corrigir erros ou mudar
seu projeto. Testes de usar quase a mesma sintaxe como especificações regra, mas os argumentos assumir ligeiramente diferentes significados. Por exemplo, o argumento endereço de origem em uma especificação regra especifica a endereço de origem que os datagramas correspondem a essa regra deve ter. O argumento de endereço de origem no syn- teste

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

fiscal, ao contrário, especifica o endereço de origem do datagrama teste que será gerado. Para `ipfwadm`, você deve usar o *-C* opção para especificar que este comando é um teste, enquanto que para `ipchains` e `IPT-veis`, Você deve usar o *-C* opção. Em todos os casos é necessário *sempre* especificar o endereço de origem, destino,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

ção de endereço, protocolo e interface a serem usados para o teste. Outros argumentos, tais como números de porta ou configurações bit TOS, são opcionais.

4. Executar cada comando de teste e observe a saída. O resultado de cada teste será uma única palavra, indicando o objectivo final do datagrama depois executá-lo através da configuração de firewall - isto é, onde o tratamento terminou. Para `ipchains` e `iptables`, Cadeias especificado pelo usuário será testado para além o built-in queridos.

5. Compare o resultado de cada teste contra o resultado desejado. Se houver alguma discrepância, será necessário para analisar o seu conjunto de regras para determinar onde você fez o erro. Caso você tenha escrito seu teste comandos em um arquivo de script, você pode facilmente executar novamente o teste depois de corrigidos os erros em sua configuração de firewall.
   É uma boa prática para lavar o seu rulesets completamente e reconstruí-los a partir do zero, ao invés de fazer muda dinamicamente. Isso ajuda a garantir que a configuração ativa você está testando na verdade, reflete a conjunto de comandos em seu script de configuração.

Vamos dar uma olhada no que uma transcrição de teste manual ficaria para o nosso exemplo ingênuo com `ipchains`. Você vai se lembrar que a nossa rede local, o exemplo foi 172.16.1.0 com uma máscara de rede 255.255.255.0 e fomos para permitir conexões TCP para servidores web na rede. Nada mais havia de passar em frente a nossa cadeia. Comece com uma transmissão que sabemos que deve funcionar, uma conexão de um host local para um servidor web fora:

```
# ipchains-C frente p tcp-s-1025-d 172.16.1.0 44.136.8.2 80-i eth0
Aceita
```

Observe os argumentos tinham de ser oferecidos ea forma como eles têm sido usados para descrever um datagrama. A saída do comando que indica que o datagrama foi aceito para a transmissão, que é o que esperávamos.

Agora, tente outro teste, desta vez com um endereço de origem que não pertencem à nossa rede. Este deve ser negada:

```
# ipchains-C frente p tcp-s-1025-d 172.16.2.0 44.136.8.2 80-i eth0
negado
```

Tente mais alguns testes, desta vez com os mesmos detalhes como o primeiro teste, mas com protocolos diferentes. Estes devem ser negado, também:

```
# ipchains-C frente p udp-s-1025-d 172.16.1.0 44.136.8.2 80-i eth0
negado
# ipchains-C frente p icmp-s-1025-d 172.16.1.0 44.136.8.2 80-i eth0
negado
```

Tente um outro porto de destino, mais uma vez esperando para ser negada:

```
# ipchains-C frente p tcp-s-1025-d 172.16.1.0 44.136.8.2 23-i eth0
negado
```

Você vai percorrer um longo caminho para alcançar a paz de espírito se você projetar uma série de testes exaustivos. Embora isso possa às vezes ser tão difícil como projetar a configuração de firewall, também é a melhor maneira de saber que seu projeto é proporcionar a segurança que você espera dele.

Uma configuração de firewall de exemplo

Nós discutimos os fundamentos da configuração do firewall. Vamos agora olhar para o que um firewall de configuração pode realmente se parecem.

A configuração neste exemplo foi projetado para ser facilmente estendido e personalizado. Nós fornecemos três versões. A primeira versão foi desenvolvida utilizando o `ipfwadm` comando (ou o `ipfwadm-wrapper` script), segundo os usos `ipchains`E os usos terceiro `iptables`. O exemplo não tentar explorar definido pelo usuário correntes, mas ele vai mostrar as semelhanças e diferenças entre a ferramenta de antigos e novos configuração do firewall sintaxes:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
#! / Bin / bash
################################################## ########################
# IPFWADM VERSÃO
# Este exemplo de configuração é para uma única configuração de firewall de host
# Sem serviços suportados pela máquina firewall.
################################################## ########################

# Seção de CONFIGURÁVEL

# O nome ea localização do utilitário ipfwadm. Use ipfwadm-wrapper para
# 2.2 .* miolo.
IPFWADM ipfwadm =

# O caminho para o ipfwadm executável.
PATH = "/ sbin /"

# Nosso espaço de endereço de rede interna e seu dispositivo de rede de apoio.
OURNET = "172.29.16.0/24"
OURBCAST = "172.29.16.255"
OURDEV = "eth0"

# O endereço externo e um dispositivo de rede que o suporta.
ANYADDR = "0 / 0"
ANYDEV = "eth1"

# Os serviços TCP queremos deixar passar - "" vazio, todas as portas
# Nota: espaço separado
TCPIN "www smtp" =
TCPOUT = "smtp www ftp irc ftp-data"

# Os serviços UDP queremos deixar passar - "" vazio, todas as portas
# Nota: espaço separado
UDPIN = "domínio"
UDPOUT = "domínio"

# Os serviços ICMP queremos deixar passar - "" vazio, todos os tipos
# Ref: / usr / include / netinet / ip_icmp.h para digitar números
# Nota: espaço separado
ICMPIN = "0 3 11"
ICMPOUT = "8 3 11"

# Log, descomente a seguinte linha para habilitar o log de datagramas
# Que são bloqueados pelo firewall.
# Logging = 1

# SECÇÃO DE USUÁRIO FINAL CONFIGURÁVEL
################################################## ########################
# Lave as regras da tabela de entrada
$ I-ipfwadm-F

# Nós queremos negar o acesso de entrada por padrão.
$ Ipfwadm-I-p negar

# Spoofing
# Não devemos aceitar os datagramas com endereço de origem correspondente a nossa
# A partir do exterior, de modo que negá-los.
$ Ipfwadm-I-a deny-S $ OURNET-W $ ANYDEV

# Smurf
# Proibir ICMP para o nosso endereço de broadcast para evitar o "Smurf" ataque estilo.
$ Ipfwadm-I-a deny-P icmp-W $ ANYDEV-D $ OURBCAST

# TCP
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# Aceitamos todos os datagramas TCP pertencentes a uma conexão existente
# (Ou seja, ter o bit ACK) para as portas TCP estamos permitindo que passar.
# Este deve pegar mais de 95% de todos os pacotes TCP válido.
$ Ipfwadm-I-a accept-P tcp-D $ OURNET $ k-TCPIN-b

# TCP - Conexões de Entrada
# Vamos aceitar pedidos de ligação a partir do exterior apenas no
# Permitiu portas TCP.
$ Ipfwadm-I-a accept-P tcp-W $ ANYDEV-D $ $ OURNET TCPIN-y

# TCP - conexões de saída
# Aceitamos todas as solicitações de conexão TCP de saída nas portas TCP permitido.
$ Ipfwadm-I-a accept-P tcp-W $ OURDEV-D $ $ ANYADDR TCPOUT-y

# UDP - INCOMING
# Vamos permitir datagramas UDP nas portas permitidas.
$ Ipfwadm-I-a accept-P udp-W $ ANYDEV-D $ $ OURNET UDPIN

# UDP - SAÍDA
# Vamos permitir que os datagramas UDP nas portas permitidas.
$ Ipfwadm-I-a accept-P udp-W $ OURDEV-D $ $ ANYADDR UDPOUT

# ICMP - INCOMING
# Vamos permitir datagramas ICMP em um dos tipos permitidos.
$ Ipfwadm-I-a accept-P icmp-W $ ANYDEV-D $ $ OURNET UDPIN

# ICMP - SAÍDA
# Vamos permitir datagramas ICMP para fora dos tipos permitidos.
$ Ipfwadm-I-a accept-P icmp-W $ OURDEV-D $ $ ANYADDR UDPOUT

# Default e registro
# Todos os datagramas restantes caem para o padrão
# Regra e são descartados. Eles serão registrados se você
# Configurado a variável LOGGING acima.
#
if ["$ REGISTRO"]
em seguida,
        # Log barrados TCP
        $ Ipfwadm-I-a rejeitar-P tcp-o

        # Log barrados UDP
        $ Ipfwadm-I-a rejeição P udp-o-

        # Log barrados ICMP
        $ Ipfwadm-I-a rejeição P icmp-o-
fi
#
# Fim.
```

Agora vamos reimplementar-lo usando o `ipchains` comando:

```
#! / Bin / bash
################################################## ########################
# Versão IPCHAINS
# Este exemplo de configuração é para uma única configuração de firewall de host
# Sem serviços suportados pela máquina firewall.
################################################## ######################

# Seção de CONFIGURÁVEL

# O nome ea localização do utilitário ipchains.
IPCHAINS = ipchains

# O caminho para o ipchains executável.
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
PATH = "/ sbin /"

# Nosso espaço de endereço de rede interna e seu dispositivo de rede de
apoio.
OURNET = "172.29.16.0/24"
OURBCAST = "172.29.16.255"
OURDEV = "eth0"

# O endereço externo e um dispositivo de rede que o suporta.
ANYADDR = "0 / 0"
ANYDEV = "eth1"

# Os serviços TCP queremos deixar passar - "" vazio, todas as portas
# Nota: espaço separado
TCPIN "www smtp" =
TCPOUT = "smtp www ftp irc ftp-data"

# Os serviços UDP queremos deixar passar - "" vazio, todas as portas
# Nota: espaço separado
UDPIN = "domínio"
UDPOUT = "domínio"

# Os serviços ICMP queremos deixar passar - "" vazio, todos os tipos
# Ref: / usr / include / netinet / ip_icmp.h para digitar números
# Nota: espaço separado
ICMPIN = "0 3 11"
ICMPOUT = "8 3 11"

# Log, descomente a seguinte linha para habilitar o log de datagramas
# Que são bloqueados pelo firewall.
# Logging = 1

# SECÇÃO DE USUÁRIO FINAL CONFIGURÁVEL
################################################## ########################
# Lave as regras da tabela de entrada
$ Input ipchains-F

# Nós queremos negar o acesso de entrada por padrão.
$ Input ipchains-P negar

# Spoofing
# Não devemos aceitar os datagramas com endereço de origem correspondente a nossa
# A partir do exterior, de modo que negá-los.
$ Ipchains-A input-s $ OURNET-i $ ANYDEV negar-j

# Smurf
# Proibir ICMP para o nosso endereço de broadcast para evitar o "Smurf" ataque estilo.
$ Ipchains-A input-p icmp-w $ ANYDEV-d $ OURBCAST negar-j

# Devemos aceitar fragmentos, no ipchains que devemos fazer isso explicitamente.
$ Ipchains-A input-f-j ACCEPT

# TCP
# Aceitamos todos os datagramas TCP pertencentes a uma conexão existente
# (Ou seja, ter o bit ACK) para as portas TCP estamos permitindo que passar.
# Este deve pegar mais de 95% de todos os pacotes TCP válido.
Tcp $ ipchains-A input-p-d $ $ OURNET TCPIN! -Y-b-j ACCEPT

# TCP - Conexões de Entrada
# Vamos aceitar pedidos de ligação a partir do exterior apenas no
# Permitiu portas TCP.
Tcp $ ipchains-A input-p-i $ ANYDEV-d $ $ OURNET TCPIN-y-j ACCEPT

# TCP - conexões de saída
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# Aceitamos todas as solicitações de saída da conexão TCP em portas TCP permitido.
Tcp $ ipchains-A input-p-i $ OURDEV-d $ $ ANYADDR TCPOUT-y-j ACCEPT

# UDP - INCOMING
# Vamos permitir datagramas UDP nas portas permitidas.
Udp $ ipchains-A input-p-i $ ANYDEV-d $ $ OURNET UDPIN-j ACCEPT

# UDP - SAÍDA
# Vamos permitir que os datagramas UDP nas portas permitidas.
Udp $ ipchains-A input-p-i $ OURDEV-d $ $ ANYADDR UDPOUT-j ACCEPT

# ICMP - INCOMING
# Vamos permitir datagramas ICMP em um dos tipos permitidos.
$ Ipchains-A input-p icmp-w $ ANYDEV-d $ $ OURNET UDPIN-j ACCEPT

# ICMP - SAÍDA
# Vamos permitir datagramas ICMP para fora dos tipos permitidos.
Icmp $ ipchains-A input-p-i $ OURDEV-d $ $ ANYADDR UDPOUT-j ACCEPT

# Default e registro
# Todos os datagramas restantes caem para o padrão
# Regra e são descartados. Eles serão registrados se você
# Configurado a variável LOGGING acima.
#
if ["$ REGISTRO"]
em seguida,
        # Log barrados TCP
        $ Ipchains-A input-p tcp-l-j reject

        # Log barrados UDP
        $ Ipchains-A input-p udp-l-j reject

        # Log barrados ICMP
        $ Ipchains-A input-p icmp-j reject-l
fi
#
# Fim.
```

Em nosso `iptables` exemplo, nós passamos a usar o `EXPECTATIVA` conjunto de regras por causa da diferença de significado da `INPUT` conjunto de regras na *netfilter* implementação. Isto tem implicações para nós, isso significa que nenhuma das regras proteger o hospedeiro próprio firewall. Para imitar com precisão os nossos `ipchains` exemplo, poderíamos replicar cada um dos nossos
regras do `INPUT` cadeia. Para maior clareza, que deixei cair todos os datagramas de entrada recebemos de nossos interface externa
em vez disso.

```
#! / Bin / bash
################################################## ########################
# Versão IPTABLES
# Este exemplo de configuração é para uma única configuração de firewall de host
# Sem serviços suportados pela máquina firewall.
################################################## ########################

# Seção de CONFIGURÁVEL

# O nome ea localização do utilitário ipchains.
iptables IPTABLES =

# O caminho para o ipchains executável.
PATH = "/ sbin /"

# Nosso espaço de endereço de rede interna e seu dispositivo de rede de apoio.
OURNET = "172.29.16.0/24"
OURBCAST = "172.29.16.255"
OURDEV = "eth0"
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# O endereço externo e um dispositivo de rede que o suporta.
ANYADDR = "0 / 0"
ANYDEV = "eth1"

# Os serviços TCP queremos deixar passar - "" vazio, todas as portas
# Nota: separados por vírgula
TCPIN = "smtp, www"
TCPOUT = "smtp, ftp, www, ftp-data, irc"

# Os serviços UDP queremos deixar passar - "" vazio, todas as portas
# Nota: separados por vírgula
UDPIN = "domínio"
UDPOUT = "domínio"

# Os serviços ICMP queremos deixar passar - "" vazio, todos os tipos
# Ref: / usr / include / netinet / ip_icmp.h para digitar números
# Nota: separados por vírgula
ICMPIN = "0,3,11"
ICMPOUT = "8,3,11"

# Log, descomente a seguinte linha para habilitar o log de datagramas
# Que são bloqueados pelo firewall.
# Logging = 1

# SECÇÃO DE USUÁRIO FINAL CONFIGURÁVEL
################################################## ##########################
# Lave as regras da tabela de entrada
Iptables-F FORWARD

# Nós queremos negar o acesso de entrada por padrão.
Iptables-P FORWARD negar

# Drop todos os datagramas destinados para este host provenientes do exterior.
Iptables-A INPUT-i $ DROP ANYDEV-j

# Spoofing
# Não devemos aceitar os datagramas com endereço de origem correspondente a nossa
# A partir do exterior, de modo que negá-los.
Iptables-A FORWARD-s $ OURNET DROP-i $ ANYDEV-j

# Smurf
# Proibir ICMP para o nosso endereço de broadcast para evitar o "Smurf" ataque estilo.
Iptables-A FORWARD-m multiport-p icmp-i $ ANYDEV-d $ OURNET NEGAR-j

# Devemos aceitar fragmentos, no iptables, devemos fazê-lo explicitamente.
Iptables-A FORWARD-m-j ACCEPT

# TCP
# Aceitamos todos os datagramas TCP pertencentes a uma conexão existente
# (Ou seja, ter o bit ACK) para as portas TCP estamos permitindo que passar.
# Este deve pegar mais de 95% de todos os pacotes TCP válido.
Tcp $ IPTABLES-A FORWARD-m multiport-p-d $ OURNET - dports $ TCPIN /
    ! - Tcp-flags SYN, ACK ACK ACCEPT-j
Iptables-A FORWARD-m multiport-p tcp-s $ OURNET - Esportes $ TCPIN /
    ! - Tcp-flags SYN, ACK ACK ACCEPT-j


# TCP - Conexões de Entrada
# Vamos aceitar pedidos de ligação a partir do exterior apenas no
# Permitiu portas TCP.
Iptables-A FORWARD-m multiport-p tcp-i $ ANYDEV-d $ $ OURNET TCPIN /
    - Syn-j ACCEPT
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# TCP - conexões de saída
# Aceitamos todas as solicitações de conexão TCP de saída do permitido /
    portas TCP.
Iptables-A FORWARD-m multiport-p tcp-i $ OURDEV-d $ ANYADDR /
    - Dports $ TCPOUT - syn-j ACCEPT
# UDP - INCOMING
# Vamos permitir datagramas UDP nas portas permitidas e volta.
Iptables-A FORWARD-m multiport-p udp-i $ ANYDEV-d $ OURNET /
    - Dports $ UDPIN-j ACCEPT
Iptables-A FORWARD-m multiport-p udp-i $ ANYDEV-s $ OURNET /
    - Desportos $ UDPIN-j ACCEPT
# UDP - SAÍDA
# Vamos permitir que os datagramas UDP para as portas permitidas e para trás.
Iptables-A FORWARD-m multiport-p udp-i $ OURDEV-d $ ANYADDR /
    - Dports $ UDPOUT-j ACCEPT
Iptables-A FORWARD-m multiport-p udp-i $ OURDEV-s $ ANYADDR /
    - Desportos $ UDPOUT-j ACCEPT
# ICMP - INCOMING
# Vamos permitir datagramas ICMP em um dos tipos permitidos.
Icmp $ IPTABLES-A FORWARD-m multiport-p-i $ ANYDEV-d $ OURNET /
    - Dports $ ICMPIN-j ACCEPT
# ICMP - SAÍDA
# Vamos permitir datagramas ICMP para fora dos tipos permitidos.
Icmp $ IPTABLES-A FORWARD-m multiport-p-i $ OURDEV-d $ ANYADDR /
    - Dports $ ICMPOUT-j ACCEPT
# Default e registro
# Todos os datagramas restantes caem para o padrão
# Regra e são descartados. Eles serão registrados se você
# Configurado a variável LOGGING acima.
#
if ["$ REGISTRO"]
em seguida,
        # Log barrados TCP
        LOG iptables-A FORWARD-m tcp-p tcp-j
        # Log barrados UDP
        LOG iptables-A FORWARD-m udp-p udp-j
        # Log barrados ICMP
        Icmp $ IPTABLES-A FORWARD-p udp-m-j LOG
fi
#
# Fim.
```

Em muitas situações simples, para usar o exemplo de tudo que você precisa fazer é editar a seção superior do arquivo

denominado "USUÁRIO
CONFIGURÁVEL seção "para especificar que tipo de datagramas e protocolos que você deseja permitir entrar e sair. Para configurações mais complexas, você precisará editar a seção na parte inferior, também. Lembre-se, esta é uma simples exemplo, para examinar com muito cuidado para garantir que ele faz o que quiser, enquanto sua aplicação.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 10 - Contabilidade IP

No mundo de hoje de serviços de Internet comercial, é cada vez mais importante saber quantos dados você está transmitindo e recebendo em suas conexões de rede. Se você é um Internet Service Provider e você cobrar de seus clientes, em volume, isso será essencial para o seu negócio. Se você é um cliente de Internet Service Provider que as taxas por volume de dados, você vai achar que é útil para coletar seus próprios dados para garantir a acu-cracia dos encargos da Internet.

Existem outros usos para a contabilização de rede que não tem nada a ver com dólares e contas. Se você gerencia um servidor que oferece um número de diferentes tipos de serviços de rede, pode ser útil para você saber exatamente como quantidade de dados está sendo gerado por cada um. Este tipo de informação pode ajudar na tomada de decisões, tais como qual hardware comprar ou quantos servidores para executar.

O kernel Linux fornece uma facilidade que permite que você reúna todos os tipos de informações úteis sobre a rede tráfego que vê. Este mecanismo é chamado *contabilidade IP*.

Configurando o kernel para Contabilidade IP

A função de contabilização Linux IP está intimamente relacionado com o software de firewall Linux. Os lugares que você quer coleta de dados contábeis são os mesmos lugares que você estaria interessado em realizar firewall de filtragem: entrada e fora de uma rede de acolhimento, e no software que faz o roteamento de datagramas. Se você ainda não leu a seção sobre firewalls, agora é provavelmente um bom momento para fazer isso, porque nós estaremos usando alguns dos conceitos descritos no Capítulo 9,
Firewall TCP / IP.

Para ativar a função de contabilização Linux IP, você deve primeiro ver se o kernel do Linux está configurado para isso. Confira para ver se o */ Proc / net / ip_acct* o arquivo já existe. Se isso acontecer, o seu kernel já suporta contabilidade IP. Se não, você deve construir um novo kernel, assegurando que você responda "Y" para as opções em kernels da série 2.0 e 2.2:

```
Networking options  --->
        [*] Os firewalls de rede
        [*] Rede TCP / IP
         ...
        [*] IP: contabilidade
```

ou em kernels 2.4 série:

```
Networking options  --->
    [*] Network packet filtering (substitui o ipchains)
```

Configurando Contabilidade IP

Porque a contabilidade IP está intimamente relacionado ao firewall IP, a mesma ferramenta foi designado para configurá-lo, de

modo
`ipfwadm`,`ipchains` ou `iptables` são usados para configurar contabilidade IP. A sintaxe deste comando é muito semelhante
para que as regras de firewall, de modo que não incidirá sobre ele, mas vamos discutir o que você consegue descobrir sobre a natureza
do seu tráfego de rede usando este recurso.

A sintaxe geral para a contabilidade de IP com `ipfwadm` é o seguinte:

```
# ipfwadm-A [direção[]comando[]parâmetros]
```

O argumento da direção é nova. Isto é simplesmente codificados como `em`,`fora`Ou `ambos`. Essas direções são do per-perspectiva da máquina linux em si, de modo `em` dados significa que entram na máquina de uma conexão de rede e `fora` significa que os dados que está sendo transmitido por este host em uma conexão de rede. A `ambos` direção é a soma de tanto na entrada quanto na saída.

A sintaxe do comando geral para `ipchains` e `iptables` é o seguinte:

```
# ipchains-A      regra da cadeia de especificação
# iptables-A      regra da cadeia de especificação
```

Ambos `ipchains` e `iptables` comandos permitem que você especificar a direção de um pacote mais coerente com a

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

regras de firewall. IP Firewall Chains não permitem que você configure uma regra que agrega ambos os sentidos, mas não

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

permitem que você configure regras do `frente` cadeia que os mais velhos não aplicação. Vamos ver as diferença que faz em alguns exemplos um pouco mais tarde.

Os comandos são praticamente as mesmas regras de firewall, exceto que as regras da política não se aplica aqui. Podemos acrescentar,
insert, delete, e regras contabilísticas lista. No caso da `ipchains` e `iptables`, Todas as regras são válidas contabilidade regras, e qualquer comando que não especifica o *-J* opção executa contabilidade só.

Os parâmetros da regra de especificação para a contabilidade de IP são os mesmos que os utilizados para firewall IP. Estes são o que nós
usar para definir precisamente o que o tráfego de rede que queremos contar e total.

Contabilidade por Endereço

Vamos trabalhar com um exemplo para ilustrar como usaríamos contabilidade IP.

Imagine que temos um roteador baseado em Linux que serve a dois departamentos na Cervejaria Virtual. O roteador tem dois dispositivos Ethernet, *eth0* e *eth1*, Cada um dos quais os serviços de um departamento e um dispositivo de PPP, *ppp0*, Que nos conecta
através de um link serial de alta velocidade para o campus principal da universidade de Groucho Marx.

Imaginemos também que, para efeitos de facturação, queremos saber o tráfego total gerado por cada um dos departamentos mentos através da ligação em série, e para efeitos de gestão, queremos saber o tráfego total gerado entre os dois departamentos.

A tabela a seguir mostra a interface endereços usaremos no nosso exemplo:

iface	endereço	netmask
eth0	172.16.3.0	255.255.255.0
eth1	172.16.4.0	255.255.255.0

Para responder à pergunta: "Como a quantidade de dados que cada departamento de gerar no link PPP?", Poderíamos usar uma regra
parecida com esta:

```
# ipfwadm-A-tanto um W-172.16.3.0/24 ppp0-S-b
# ipfwadm-A-tanto um W-172.16.4.0/24 ppp0-S-b
```

ou:

```
# ipchains-A input-i ppp0-d 172.16.3.0/24
# ipchains-A saída-i ppp0-s 172.16.3.0/24
# ipchains-A input-i ppp0-d 172.16.4.0/24
# ipchains-A saída-i ppp0-s 172.16.4.0/24
```

e com `iptables`:

```
# iptables-A FORWARD-i ppp0-d 172.16.3.0/24
# iptables-A FORWARD-o ppp0-s 172.16.3.0/24
# iptables-A FORWARD-i ppp0-d 172.16.4.0/24
# iptables-A FORWARD-o ppp0-s 172.16.4.0/24
```

A primeira metade de cada uma dessas conjunto de regras dizem: "Contar todos os dados que viajam em qualquer direção através da interface
chamada ppp0 com origem ou destino (lembre-se a função do *-B* bandeira `ipfwadm` e `iptables`) endereço do `172.16.3.0/24`."O segundo semestre de cada conjunto de regras é o mesmo, mas para a rede Ethernet de segunda
trabalho em nosso site.

Para responder à segunda questão, "quanto os dados trafegam entre os dois departamentos?", Precisamos de uma regra que parecido com este:

```
# ipfwadm-A-172.16.4.0/24 tanto uma S-172.16.3.0/24-b-D
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

ou:
ipchains-A FORWARD-s 172.16.3.0/24-d 172.16.4.0/24-b
ou:
iptables-A FORWARD-s 172.16.3.0/24-d 172.16.4.0/24
iptables-A FORWARD-s 172.16.4.0/24-d 172.16.3.0/24

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Estas regras vão contar todos os datagramas com endereço de origem pertencente a uma das redes de departamento e um
endereço de destino pertence ao outro.

Contabilidade pela porta de serviço

Ok, vamos supor que nós também queremos uma melhor idéia de exatamente que tipo de tráfego está sendo realizado através de nosso link PPP.
Poderíamos, por exemplo, quer saber quanto do link FTP, SMTP, e serviços na World Wide Web são consumindo.

Um script de regras que nos permitam recolher essa informação pode parecer:

```
#! / Bin / sh
# Coletar FTP, SMTP e as estatísticas de volume de dados www realizado em nosso
# Ligação PPP usando ipfwadm
#
ipfwadm-A-tanto um W-ppp0-P tcp-S 0 / 0 ftp ftp-data
ipfwadm-A-tanto um W-ppp0-P tcp-S 0 / 0 smtp
ipfwadm-A-tanto um W-ppp0-P tcp-S 0 / 0 www
```

ou:

```
#! / Bin / sh
# Coletar FTP, SMTP e as estatísticas de volume de dados www realizado em nosso
# Ligação PPP usando ipchains
#
ipchains-A input-i ppp0-p tcp-s 0 / 0 ftp dados: FTP
ipchains-A saída-i ppp0-p tcp-d 0 / 0 ftp dados: FTP
ipchains-A input-i ppp0-p tcp-s 0 / 0 smtp
ipchains-A saída-i ppp0-p tcp-d 0 / 0 smtp
ipchains-A input-i ppp0-p tcp-s 0 / 0 www
ipchains-A saída-i ppp0-p tcp-d 0 / 0 www
```

ou:

```
#! / Bin / sh
# Coletar FTP, SMTP e as estatísticas de volume de dados www realizado em nosso
# Iptables ligação PPP usando.
#
iptables-A FORWARD-i ppp0-m tcp-p tcp - sport ftp dados: FTP
iptables-A FORWARD-o ppp0-m tcp-p tcp - dport ftp dados: FTP
iptables-A FORWARD-i ppp0-m tcp-p tcp - smtp esporte
iptables-A FORWARD-o ppp0-m tcp-p tcp - dport smtp
iptables-A FORWARD-i ppp0-m tcp-p tcp - sport www
iptables-A FORWARD-o ppp0-m tcp-p tcp - dport www
```

Há um par de características interessantes para esta configuração. Em primeiro lugar, temos o protocolo especificado. Quando nós
especifique as portas nas nossas regras, nós também deve especificar um protocolo TCP e UDP, pois fornecem conjuntos separados de portas.
Uma vez que todos estes serviços estão baseados TCB, nós especificou como o protocolo. Em segundo lugar, temos os dois especificado
serviços `ftp` e `ftp-data` em um comando. `ipfwadm` permite que você especificar portas individuais, intervalos de portas, ou listas arbitrárias dos portos. A `ipchains` comando permite que as portas simples ou intervalos de portas, que é o que usamos aqui. A sintaxe "`ftp-data: ftp`"Significa" portas ftp-data (20) através de FTP (21), "e é como nós intervalos de codificar de portas em ambos os `ipchains` e `iptables`. Quando você tem uma lista de portas em uma regra de contabilidade,
isso significa que os dados recebidos para qualquer um dos portos da lista fará com que os dados sejam adicionados aos totais dessa entrada.
Lembrando que o serviço FTP usa duas portas, a porta de comando ea porta de transferência de dados, nós adicionamos juntos para o total do tráfego FTP. Finalmente, tenha especificado o endereço de origem como "`0 / 0,`"Que é especial notação que corresponde a todos os endereços e é requerido por ambos os `ipfwadm` e `ipchains` comandos, a fim de especificar portas.

Podemos expandir o segundo ponto um pouco para nos dar uma visão diferente dos dados em nosso link. Vamos agora imaginar que classe FTP, SMTP e World Wide Web tráfego como o tráfego essencial, e todos os outros tráfegos como não essenciais. Se estávamos interessados em ver a relação de tráfego essencial para o tráfego não essencial, poderíamos fazer algo como:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
#  ipfwadm-A-tanto um W-ppp0-P tcp-S 0 / 0 FTP, SMTP dados ftp-www
#  ipfwadm-A-tanto um W-ppp0-P tcp-S 0 / 0 1:19 22:24 26:79 81:32767
```

Se você já analisou o seu */ Etc / services* arquivo, você verá que a segunda regra abrange todas as portas exceto (`ftp`,`ftp-data`,`smtp`E `www`).

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Como podemos fazer isso com o `ipchains` ou `iptables` comandos, uma vez que permitem apenas um argumento em suas especificação da porta? Podemos explorar cadeias definidas pelo usuário em contabilidade tão facilmente como em regras de firewall. Considere
a seguinte abordagem:

```
# ipchains-N um essenc-
# ipchains-N um noness-
# ACCEPT ipchains-A a-essenc-j
# ACCEPT ipchains-A a-noness-j
# ipchains-A FORWARD-i ppp0-p tcp-s 0 / 0 ftp dados: ftp-j uma importânc-
# ipchains-A FORWARD-i ppp0-p tcp-s 0 / 0 smtp-j uma importânc-
# ipchains-A FORWARD-i ppp0-p tcp-s 0 / 0 www-j uma importânc-
# ipchains-A forward-j um noness-
```

Aqui criamos duas cadeias definidas pelo usuário, um chamado `uma importânc-`, Onde a captura de dados essenciais para a contabilidade
serviços e um outro chamado `um noness-`, Onde a captura de dados contábeis para os serviços não essenciais. Em seguida, adicionar regras para a nossa cadeia de transmitir a que correspondem os nossos serviços essenciais e saltar para a `uma importânc-` cadeia, onde
tem apenas uma regra que aceite todos os datagramas e conta-los. A última regra em nossa cadeia de frente é uma regra que salta para o nosso `um noness-` cadeia, onde, novamente, temos apenas uma regra que aceite todos os datagramas e conta-los. A regra que salta para o `um noness-` corrente não será alcançado por qualquer dos nossos serviços essenciais, como eles vão ter sido aprovado em sua própria cadeia. Nossa registra para os serviços essenciais e não essenciais, portanto, ser dis-
poder nas regras dentro dessas cadeias. Esta é apenas uma abordagem que poderia tomar, existem outros. Nossa `iptables` aplicação da mesma abordagem seria algo como:

```
# iptables-N um essenc-
# iptables-N um noness-
# ACCEPT iptables-A a-essenc-j
# ACCEPT iptables-A a-noness-j
# iptables-A FORWARD-i ppp0-m tcp-p tcp - sport ftp dados: ftp-j a-
essenc
# iptables-A FORWARD-i ppp0-m tcp-p tcp - smtp-j um esporte essenc-
# iptables-A FORWARD-i ppp0-m tcp-p tcp - sport www-j uma importânc-
# iptables-A FORWARD-j um noness-
```

Isso parece bastante simples. Infelizmente, há um pequeno problema, mas inevitável quando se tenta fazer uma contabilidade por tipo de serviço. Você vai se lembrar que nós discutimos o papel que a MTU joga em rede TCP / IP em uma versão anterior capítulo. A MTU define o maior datagrama que serão transmitidos em um dispositivo de rede. Quando um datagrama é
recebido por um roteador que é maior que a MTU da interface de que necessita para retransmiti-lo, o roteador realiza um truque chamado *fragmentação*. O roteador divide o datagrama grande em pedaços pequenos não mais do que a MTU da interface e, em seguida, transmite essas peças. O roteador constrói novos cabeçalhos para colocar na frente de cada uma dessas peças,
e estes são o que o computador remoto usa para reconstruir os dados originais. Infelizmente, durante a fragmen-
processo de mediação que a porta está perdido para todos, mas o primeiro fragmento. Isto significa que a contabilidade IP não pode contar corretamente
datagramas fragmentados. Ele pode confiantemente contar apenas o primeiro fragmento, ou datagramas não fragmentados. Há uma pequena
truque permitido pela `ipfwadm` que garante que enquanto não seremos capazes de saber exatamente o que a porta do segundo e fragmentos foram depois de, ainda podemos contá-los. Uma versão inicial do Linux software de contabilidade atribuído o fragmentos de um número de porta falsa, 0xFFFF, que podemos contar. Para garantir que captura o segundo e mais tarde fragmentos, podemos usar uma regra como:

```
# ipfwadm-A-tanto um W-ppp0-P tcp-S 0 / 0 0xFFFF
```

O IP execução cadeias tem uma solução um pouco mais sofisticado, mas o resultado é praticamente o mesmo. Se estiver usando o `ipchains` comando que usaria:

```
# ipchains-A FORWARD-i ppp0-p tcp-m
```

e com `iptables` usaríamos:

```
# iptables-A FORWARD-i ppp0-m tcp-p tcp-m
```

Estes não vão nos dizer o que o porto original de dados foi, mas pelo menos somos capazes de ver o quanto de nossos dados é fragmentos, e ser capaz de dar conta do volume de tráfego que eles consomem.

No kernel 2.2 você pode selecionar uma opção do kernel em tempo de compilação, que nega toda esta questão se a sua máquina

Linux
atuando como o único ponto de acesso para uma rede. Se você ativar o *IP: sempre desfragmentar* opção quando com-
monte o seu kernel, todos os datagramas recebidos serão reagrupados pelo roteador Linux antes do roteamento e retransmissão,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Sion. Esta operação é realizada antes que o software de firewall e de contabilidade vê o datagrama, e assim você não terá de lidar com fragmentos. No kernel 2.4 você compilar e carregar o *netfilter forward-fragmento* módulo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Contabilidade de datagramas ICMP

O protocolo ICMP não utiliza números de porta de serviço e por isso é um pouco mais difícil coletar informações em. ICMP usa um número de diferentes tipos de datagramas. Muitos deles são inofensivos e normais, enquanto outros devem ser vistos apenas em circunstâncias especiais. Às vezes as pessoas com muito tempo nas mãos tentativa maliciosamente para interromper o acesso à rede de um usuário, gerando um grande número de mensagens ICMP. Esta é comumente chamado *inundações ping*. Embora a contabilização IP não pode fazer nada para evitar esse problema (IP firewall pode ajudar, embora!), podemos pelo menos colocar as regras contabilísticas em vigor que vai nos mostrar se alguém tem tentado.

ICMP não usa as portas TCP e UDP como fazer. Em vez disso ICMP tem tipos de mensagens ICMP. Nós podemos construir

regras para
conta para cada tipo de mensagem ICMP. Para fazer isso, nós colocamos a mensagem ICMP tipo e número no lugar do no campo da porta `ipfwadm` comandos de contabilidade. Listamos os tipos de mensagens ICMP "datagrama ICMP tipos ", para se referir a ele, se você precisa se lembrar que eles são.

Uma regra de contabilidade IP para coletar informações sobre o volume de dados ping que está sendo enviado a você ou que

você
estão gerando pode parecer:

```
#  ipfwadm-A-um-tanto-P icmp-S 0 / 0 8
#  ipfwadm-A-um-tanto-P icmp-S 0 / 0 0
#  ipfwadm-A-um-tanto-P icmp-S 0 / 0 0xff
```

ou, com `ipchains`:

```
#  ipchains-A FORWARD-p icmp-s 0 / 0 8
#  ipchains-A FORWARD-p icmp-s 0 / 0 0
#  ipchains-A FORWARD-p icmp-s 0 / 0-f
```

ou, com `iptables`:

```
#  iptables-A FORWARD-m icmp p icmp - echo-request esportes
#  iptables-A FORWARD-m icmp p icmp - echo-reply esportes
#  iptables-A FORWARD-p icmp-m icmp-f
```

A primeira regra coleta informações sobre a "solicitação de eco ICMP" datagramas (os pedidos ping), eo segundo Estado recolhe informações sobre o "ICMP echo reply" datagramas (respostas de ping). A terceira regra coleta informações sobre fragmentos de datagramas ICMP. Este é um truque semelhante à descrita para TCP e UDP fragmentados datagramas.

Se você especificar a fonte e / ou endereços de destino nas suas regras, você pode acompanhar onde os pings estão discussão de, como se se originam dentro ou fora da rede. Depois de determinar que o
datagramas desonestos estão vindo, você pode decidir se você quer colocar regras de firewall para prevenir los ou tomar alguma outra ação, como entrar em contato com o proprietário da rede de ofender a aconselhá-los da problema, ou talvez até mesmo ação legal, caso o problema é um ato malicioso.

Contabilidade pelo Protocolo

Vamos agora imaginar que estamos interessados em saber o quanto de tráfego em nosso link é TCP, UDP e ICMP. Gostaríamos de usar as regras como a seguinte:

```
#  ipfwadm-A-tanto um W-ppp0-P tcp-D 0 / 0
#  ipfwadm-A-tanto um W-ppp0-P udp-D 0 / 0
#  ipfwadm-A-tanto um W-ppp0-P icmp-D 0 / 0
```

ou:

```
#  ipchains-A FORWARD-i ppp0-p tcp-d 0 / 0
#  ipchains-A FORWARD-i ppp0-p udp-d 0 / 0
#  ipchains-A FORWARD-i ppp0-p icmp-d 0 / 0
```

ou:

```
#  iptables-A FORWARD-i ppp0-m tcp-p tcp
#  iptables-A FORWARD-o ppp0-m tcp-p tcp
#  iptables-A FORWARD-i ppp0-m udp p udp-
#  iptables-A FORWARD-o ppp0-m udp p udp-
#  iptables-A FORWARD-i ppp0-m icmp p icmp-
#  iptables-A FORWARD-o ppp0-m icmp p icmp-
```

Com estas regras em vigor, todo o tráfego flui através do `ppp0` interface será analisada para determinar se é TCP, UDP, ou tráfego IMCP, e os contadores apropriados será atualizado para cada um. A `iptables` exemplo, diferencia o fluxo de entrada de fluxo de saída como sua sintaxe exige.

PDF Creator PDF4Free v2.0 http://www.pdf4free.com

Usando os resultados contábeis IP

É muito fácil estar a recolher essa informação, mas como é que vamos realmente começar a ver isso? Para visualizar o

recolhidos
dados contábeis e as normas contabilísticas configurados, usamos nossos comandos de configuração de firewall, pedindo-lhes para listar as nossas regras. Os contadores de pacotes e bytes para cada uma das nossas regras são listadas na saída.

A `ipfwadm`,`ipchains`E `iptables` comandos diferem na forma como os dados contabilísticos sejam tratadas, por isso

vamos
tratá-los de forma independente.

Listagem de Dados Contábeis com ipfwadm

A forma mais básica de listagem dos dados contábeis com o `ipfwadm` comando é usá-lo como este:

```
# l ipfwadm-A-
regras contabilísticas IP
 pkts bytes fonte prot dir                destino              portas
 9833 2345K i / o todos os              em qualquer lugar    n / a
                     172.16.3.0/24      em qualquer lugar    n / a
56527   33M / S Todos os  172.16.4.0/24
```

Isto irá dizer-nos o número de pacotes enviados em cada direção. Se usamos o formato de saída ampliada com a *-E* opção (não mostrado aqui, pois a saída é muito grande para a página), que também são fornecidas as opções e apli- interface nomes cabo. A maioria dos campos na saída será auto-explicativo, mas as seguintes não poderão:

dir

A direção na qual a regra se aplica. Os valores esperados estão aqui `em`,`fora`Ou `i / o`, Ou seja, nos dois sentidos.

prot

Os protocolos a que a regra se aplica.

opt

Uma forma codificada, das opções que usamos quando invocando `ipfwadm`.

ifname

O nome da interface à qual a regra se aplica.

ifaddress

O endereço da interface à qual a regra se aplica.

Por padrão, `ipfwadm` exibe os pacotes e bytes em uma forma abreviada, arredondado para o milhar mais próxima
(K) ou milhões de euros (M). Podemos pedir para ele exibir os dados coletados em unidades exatas usando a opção expandido como
seguinte forma:

```
# ipfwadm-A-l-e-x
```

Listagem de Dados Contábeis com ipchains

A `ipchains` comando não irá exibir os dados da nossa contabilidade (contadores de pacotes e bytes), a menos que a sua

apresentação
o `-V` argumento. O meio mais simples de listar os dados contábeis com o `ipchains` é usá-lo como este:

```
# ipchains-L-v
```

Novamente, assim como com `ipfwadm`, Podemos mostrar o pacote e os contadores de bytes em unidades usando a saída

ampliada
modo. A `ipchains` usa o `-X` argumento para isso:

```
# ipchains-L-v-x
```

Listagem de Dados Contábeis com iptables

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A `iptables` comando se comporta de forma muito semelhante à `ipchains` comando. Novamente, é preciso usar o `-V` quando as regras do tour anúncio para ver os contadores de contabilidade. Para listar os dados da nossa contabilidade, devemos usar:

```
# iptables-L-v
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Assim como para o `ipchains` comando, você pode usar o `-X` argumento para mostrar a saída em formato ampliado com valores unitários.

Redefinindo os contadores

Os contadores de contabilidade IP vai transbordar se você deixá-los por muito tempo. Se transbordar, vai ter dificuldade determinar o valor que eles realmente representam. Para evitar esse problema, você deve ler os dados contábeis periodicamente, gravar, e depois repor os contadores de volta a zero para começar a coleta de informações contábeis para o intervalo contabilístico seguinte.

A `ipfwadm` e `ipchains` comandos de lhe proporcionar um meio de fazer isso simplesmente:

```
# ipfwadm-A-z
```

ou:

```
# ipchains-Z
```

ou:

```
# iptables-Z
```

Você pode até combinar a lista e zerar as ações em conjunto para garantir que nenhum dado é perdido na contabilidade entre:

```
# l ipfwadm-A-z
```

ou:

```
# ipchains-L-Z
```

ou:

```
# iptables-L-v-Z
```

Estes comandos primeira lista os dados contábeis e logo em seguida os contadores a zero e começar a contagem novamente. Se você está interessado em recolher e utilizar essas informações regularmente, você provavelmente deseja colocar este comando em um script que registrou a saída e é armazenado em algum lugar, e executar o script periodicamente usando o `cron` comando.

Rubor nas Regras

Um último comando que pode ser útil lhe permite descarregar todas as regras contabilísticas IP que você configurou. Este é mais útil quando você quer alterar radicalmente o seu conjunto de regras sem reiniciar a máquina.

A `-F` argumento em conjunto com o `ipfwadm` comando irá liberar todas as regras do tipo que você especificar. `ipchains` apoia a `-F` argumento, que faz o mesmo:

```
# ipfwadm-A-f
```

ou:

```
# ipchains-F
```

ou:

```
# iptables-F
```

Isso libera todas as suas regras contabilísticas IP configurado, removendo todos eles e de poupança que você tenha que remover cada um deles individualmente. Note que as regras de lavagem com `ipchains` não causa nenhum cadeias definidas pelo usuário para ser retirada, só as regras dentro deles.

Passivo Coleta de Dados Contábeis

Um último truque que você pode querer considerar: se a sua máquina Linux está conectado a uma rede Ethernet, você pode aplicar-AC regras de contagem de todos os dados do segmento, não só aquilo que é transmitido por ou destinadas a ele. Seu máquina passivamente ouvir todos os dados sobre o segmento e contá-lo.

Você deve primeiro ativar o encaminhamento IP em sua máquina Linux para que ele não tenta a rota datagramas que recebe.[65] n os kernels 2.0.36 e 2.2, esta é uma questão de:

```
# echo 0> / proc/sys/net/ipv4/ip_forward
```

[65] Esta não é uma boa coisa a fazer se a sua máquina Linux serve como um roteador. Se você desativar IP encaminhamento, ela deixará de rota! Faça isso apenas

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

na

uma máquina com uma única interface de rede física.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Você deve então ativar o modo promíscuo na sua interface Ethernet usando o `ifconfig` comando. Agora você pode estabelecer regras de contabilidade que lhe permitem coletar informações sobre os datagramas fluindo através de seu Ethernet sem envolver o Linux na rota de todo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 11 - Masquerade e Network Address Translation

Você não tem que ter uma boa memória para lembrar de uma época, quando apenas as grandes organizações podem dar ao luxo

de ter um
número de computadores ligados em rede por uma LAN. tecnologia de rede hoje caiu muito de preço
que duas coisas aconteceram. Primeiro, as LANs são agora comuns, mesmo em ambientes domésticos muitos. Cer-
Certamente que muitos usuários de Linux têm dois ou mais computadores conectados por alguns Ethernet. Em segundo lugar, re-rede
fontes, especialmente os endereços IP são um recurso escasso, enquanto que costumava ser livre, eles estão agora a ser comprados e vendidos.

A maioria das pessoas com uma LAN, provavelmente, também quero uma ligação à Internet que cada computador na rede local

pode
uso. O roteamento IP regras são bastante rígidas na forma como eles lidam com esta situação. As soluções tradicionais para esse problema
teria envolvido solicitando um endereço IP de rede, talvez um endereço de classe C para sites pequenos, atribuindo a cada host na rede um endereço a partir desta rede e usar um roteador para se conectar a LAN à Internet.

Em um ambiente de Internet comercializada, isto é um proposition caro. Primeiro, você seria obrigado a pagar
para o endereço de rede que é atribuído a você. Em segundo lugar, você provavelmente vai ter que pagar o seu Internet Service Pro-
se esvaziar o privilégio de ter uma rota adequada à sua rede postas em prática para que o resto da Internet
sabe como chegar até você. Isso ainda pode ser prático para as empresas, mas as instalações domésticas geralmente não justificar o custo.

Felizmente, o Linux fornece uma resposta para esse dilema. Esta resposta envolve um componente de um grupo de ad-
características avançadas de rede chamado *Network Address Translation* (NAT). NAT descreve o processo de modificar-
ção da rede de endereços contidos com cabeçalhos datagrama enquanto estão em trânsito. Isto pode soar estranho à primeiro, mas vamos mostrar que é ideal para resolver o problema que acabamos de descrever e muitos têm encontrado. IP Masquerade é o nome dado a um tipo de tradução de endereços de rede que permite que todos os hosts em uma privada rede para usar a Internet pelo preço de um único endereço IP.

Mascaramento de IP permite que você use um privado (reservado) de endereço de rede IP em sua rede e ter seu Linux
roteador baseado executar alguma tradução, inteligente em tempo real de endereços IP e portas. Quando ele recebe um datagrama
a partir de um computador na LAN, ele toma conhecimento do tipo de datagrama é, "TCP", "UDP", "ICMP", etc, e modi-
FIES o datagrama de forma que parece que ele foi gerado pela máquina próprio roteador (e lembra que ele tem
feito isso). Ele então transmite os datagramas para a Internet com o seu único endereço IP conectado. Quando o destino,
ção de acolhimento recebe esse datagrama, ele acredita que o datagrama chegou a partir do host de roteamento e envia qualquer resposta
datagramas de volta para aquele endereço. Quando o roteador Linux masquerade recebe um datagrama de sua conexão à Internet
ção, ele procura na sua tabela de estabelecer conexões mascaradas para ver se este datagrama na verdade pertence a um
computador da LAN, e se isso acontecer, ele inverte a modificação que fez no caminho para a frente e transmite o datagrama para o computador da LAN.

Um exemplo simples é ilustrado na Figura 11.1.

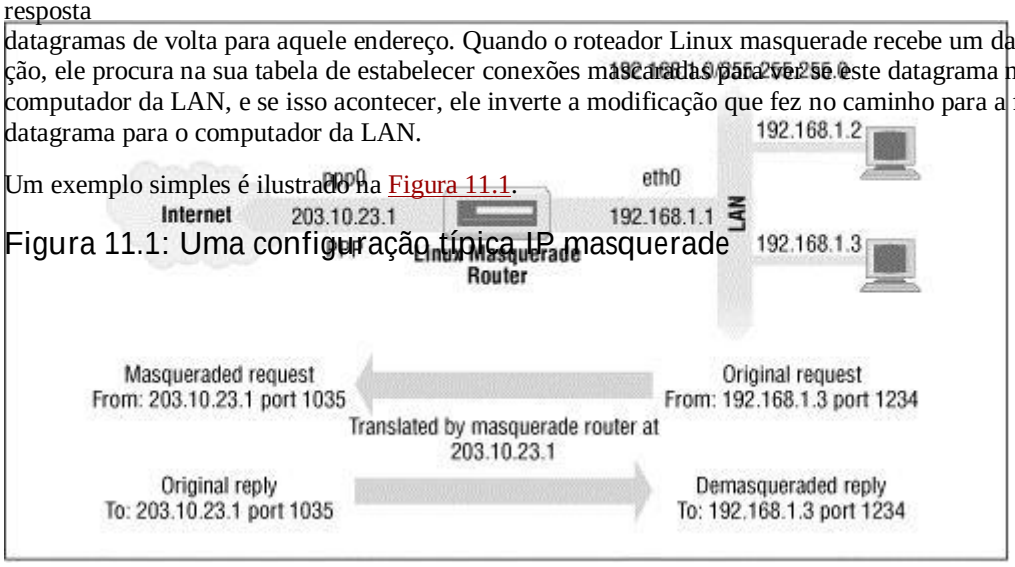


Figura 11.1: Uma configuração típica IP masquerade

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Temos uma pequena rede Ethernet usando um dos endereços de rede reservados. A rede tem um baseado em Linux mascarada roteador de acesso à Internet. Uma das estações de trabalho na rede (192.168.1.3) desejos para estabelecer uma conexão para o host remoto 209.1.106.178 na porta 8888. As rotas a sua estação de trabalho datagrama para o roteador de máscaras, que identifica o pedido de conexão como necessitando de serviços de máscaras. Ela aceita a datagrama e atribui um número de porta para usar (1035), substitui o seu próprio endereço IP eo número da porta para aqueles de o host de origem, e transmite o datagrama para o host de destino. O host de destino acredita que tem re- percebida uma solicitação de conexão do host masquerade Linux e gera um datagrama resposta. O baile de máscaras acolhimento, ao receber esse datagrama, encontra a associação em sua tabela de máscaras e inverte a substituição ao que realizada no datagrama. Em seguida, ele transmite o datagrama de resposta para o host de origem.

A máquina local acredita que está falando diretamente para o host remoto. O host remoto não sabe nada sobre o local acolhimento a todos e acredita ter recebido uma ligação a partir do host masquerade Linux. O anfitrião masquerade Linux sabe que esses dois hosts estão falando entre si, e em quais portas, e executa a tradução de endereço e porta- ções necessárias para permitir a comunicação.

Isso tudo pode parecer um pouco confuso, e pode ser, mas funciona e é realmente muito simples de configurar. Portanto, não se preocupe se você não entender todos os detalhes ainda.

Efeitos colaterais e benefícios

A facilidade mascarada IP vem com seu próprio conjunto de efeitos secundários, alguns dos quais são úteis e alguns dos quais pode tornar-se incómodo.

Nenhum dos hosts da rede suportada por trás do roteador máscaras estão sempre visto diretamente, conseqüentemente, você só precisa de um válido e roteável endereço IP para permitir que todos os hosts da rede para fazer ligações para fora no Internet. Isso tem um lado negativo, nenhum desses hosts são visíveis a partir da Internet e você não pode se conectar diretamente a los a partir da Internet, o acolhimento visível apenas em uma rede mascarada é a máquina de disfarce em si. Esta é importante quando você considera serviços como e-mail ou FTP. Ele ajuda a determinar que serviços devem ser prestados pelo acolhimento de máscaras e que serviços ele deve proxy ou tratar especialmente.

Segundo, porque nenhum dos hosts mascarados são visíveis, eles são relativamente protegido dos ataques de fora lado, o que poderia simplificar ou mesmo eliminar a necessidade de configuração do firewall no host mascarada. Você não deve confiar demais sobre isso, porém. Toda a rede será tão seguro quanto seu anfitrião masquerade, para você deve usar firewall para protegê-lo se a segurança é uma preocupação.

Em terceiro lugar, IP mascarado terá algum impacto sobre o desempenho de sua rede. Em configurações típicas este será, provavelmente, dificilmente mensurável. Se você tem um grande número de sessões ativas mascarada, porém, você pode achar que o processamento necessário para a máquina de máscaras começa a ter impacto na sua taxa de transferência de rede. IP mascarada deve fazer uma boa quantidade de trabalho para cada datagrama em relação ao processo convencional de roteamento. Essa máquina 386SX16 você foi pensando em usar como uma máquina de máscaras apoiar uma conexão dial-up Internet pode ser ótimo, mas não espere muito se você decidir que quer usá-lo como um roteador em sua empre- Taxa de rede Ethernet a velocidades.

Por último, alguns serviços de rede simplesmente não funcionará por meio de máscaras, ou pelo menos não sem muita ajuda.

Normalmente, estes são serviços que dependem de sessões de entrada para o trabalho, como alguns tipos de Comunicações diretas Chan- Nels (DCC), recursos no IRC, ou certos tipos de serviços de áudio e vídeo multicast. Alguns destes serviços têm desenvolvido especialmente os módulos do kernel para fornecer soluções para estes, e vamos falar sobre aqueles em um momento.
Para outros, é possível que você não encontrará apoio, para estar ciente de que não será adequado em todas as situações.

Configurando o kernel para o IP Masquerade

Para usar o recurso de máscaras de IP, o seu kernel deve ser compilado com o apoio de máscaras. Você deve selecionar o seguintes opções ao configurar um kernel da série 2.2:

```
Networking options  --->
        [*] Os firewalls de rede
        [*] Rede TCP / IP
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
[*] IP: firewall
[*] IP: masquerading
```

```
        --- Protocolo específico de apoio disfarçado será construído como
REGRAS. mod-

        [*] IP: apoio máscara ipautofw
        [*] IP: ICMP masquerading
```

Note-se que parte do apoio masquerade só está disponível como um módulo do kernel. Isso significa que você deve assegurar que você "`make modules`"Para além do habitual"`make zImage`"Ao construir o seu kernel.

A série de kernels 2.4 deixará de oferecer suporte a IP masquerade como uma opção de tempo de compilação de kernel. Em vez disso, você
deve selecionar a opção de filtragem de pacotes:

```
Networking options  --->
    [M] Network packet filtering (substitui o ipchains)
```

No kernel 2.2 série, uma série de módulos auxiliares específica de protocolo é criado durante a compilação do kernel. Alguns protocolos de começar com uma solicitação de saída em uma porta, e então esperar que uma conexão de entrada em outro. Normalmente, estes não podem ser mascarados, como não há nenhuma maneira de associar a segunda conexão com o primeiro sem olha dentro dos próprios protocolos. Os módulos auxiliares fazem exatamente isso, eles realmente olhar dentro do datagramas e permitir que aparece para trabalhar protocolos suportados que de outra forma seriam impossíveis de mas-querade. Os protocolos suportados são:

Módulo	Protocolo
ip_masq_ftp	FTP
ip_masq_irc	IRC
ip_masq_raudio	RealAudio
ip_masq_cuseeme	CU-See-Me
ip_masq_vdolive	Para VDO Live
ip_masq_quake	Quake é IdSoftware

Você deve carregar os módulos manualmente utilizando o `insmod` comando para implementá-los. Note que estes mod-ules não pode ser carregado utilizando o `kerneld` daemon. Cada um dos módulos tem um argumento especificando o que portos que irá ouvir. Para o RealAudio (TM) módulo que você pode usar:[66]

```
#  insmod portas ip_masq_raudio.o = 7070,7071,7072
```

As portas que você precisa especificar depende do protocolo. Um baile de máscaras IP mini-HOWTO escrito por Ambrose Au explica mais sobre os módulos masquerade IP e como configurá-los.[67]

A *netfilter* pacote inclui os módulos que desempenham funções semelhantes. Por exemplo, para fornecer conexão via
ção de sessões FTP, você pode carregar e usar o *ip_conntrack_ftp* e *ip_nat_ftp.o* módulos.

Configurando o IP Masquerade

Se você já leu os capítulos de firewall e de contabilidade, que provavelmente vem como nenhuma surpresa que o `ipfwadm`, `ipchains`E `iptables` comandos são usados para configurar as regras IP masquerade também.

Masquerade regras são uma classe especial da regra de filtragem. Você pode apenas mascarar os datagramas que são recebidos em
uma interface que vai ser encaminhado para outra interface. Para configurar uma regra de masquerade você criar uma regra muito
semelhante a uma regra de redirecionamento do firewall, mas com opções especiais que informam o kernel para mascarar o datagrama.

A `ipfwadm` usa o comando *M* opção, `ipchains` usa `MASQ-j`E `iptables` usa `J-Masquer-ADE` para indicar que os datagramas acordo com a especificação regra deve ser mascarados.

Vejamos um exemplo. Um estudante de ciência da computação na Universidade de Groucho Marx tem uma série de

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

computadores
em casa interconectados em uma rede pequena área baseada em Ethernet local. Ela optou por usar um dos re-

66 RealAudio é uma marca comercial da Progressive Networks Corporation.
67 Você pode entrar em contato com Ambrósio *ambrose@writeme.com*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

servido endereços de rede privada da internet para sua rede. Ela compartilha sua acomodação com outros estudantes, todos os de quem tem interesse em utilizar a Internet. Por causa das condições de vida do estudante são muito frugal, não podem dar ao luxo de utilizar uma ligação permanente à Internet, então em vez disso, use um simples dial-up PPP ligação à Internet. Todos eles gostariam de ser capazes de compartilhar a conexão com o bate-papo no IRC, navegar na Web, e recuperar arquivos por FTP
diretamente a cada um dos seus computadores - IP masquerade é a resposta.

O primeiro aluno configura uma máquina Linux para apoiar a conexão dial-up e para atuar como um roteador para a LAN. A endereço IP que é atribuído quando ela disca não é importante. Ela configura o roteador Linux com IP mascarado e usa um dos endereços de rede privada de seu LAN: `192.168.1.0`. Ela garante que cada um dos hosts na LAN tem uma rota default apontando para o roteador Linux.

Os seguintes `ipfwadm` comandos são todos que são obrigados a fazer o trabalho que aparece em sua configuração:

```
# ipfwadm-F-p deny
# ipfwadm-F-a accept-m-S 192.168.1.0/24-D 0 / 0
```

ou com `ipchains`:

```
# ipchains-P forward-j negar
# ipchains-A FORWARD-s 192.168.1.0/24-d 0 MASQ / 0-j
```

ou com `iptables`:

```
# iptables-t nat-P POSTROUTING DROP
# iptables-t nat-A POSTROUTING MASQUERADE-o ppp0-j
```

Agora, sempre que qualquer um dos hosts da LAN tenta se conectar a um serviço em um host remoto, o seu datagramas será auto-
automaticamente mascarados pelo roteador masquerade Linux. A primeira regra em cada exemplo, impede que o ma-Linux chine do roteamento de qualquer outros datagramas e também adiciona um pouco de segurança.

Para listar as regras de máscaras que você criou, use o `-L` argumento para o `ipfwadm` comando, como descrevemos na anterior ao discutir firewalls.

Para listar a regra que criou anteriormente usamos:

```
# ipfwadm-F-l e-
```

que deve mostrar algo como:

```
# ipfwadm-F-l e-
firewall IP regras para a frente, a política padrão: aceitar
 tipo pkts bytes  prot opt  ifname tosa tosx  ifaddress  ...
    0     0 ACC / m todos   ---- 0x00 0xff    qualquer   ...
          qualquer
```

A "`/ M`"Na saída indica que esta é uma regra de máscaras.

Para listar as regras de máscaras com o `ipchains` comando, use o `-L` argumento. Se nós listamos a regra que criamos anteriormente com `ipchains`, A saída será algo parecido com:

```
# Ipchains-L
Chain INPUT (política ACCEPT):
Chain FORWARD (política ACCEPT):
alvo       prot opt     fonte               destino             portas
MASQ       todos        ------              em qualquer lugar   n / a
                192.168.1.0/24

Cadeia de saída (política ACCEPT):
```

Todas as regras com o objectivo de `MASQ` são regras de

máscaras.

Finalmente, para listar as regras de uso `iptables` você

precisa usar:

```
# iptables-t nat-L
Chain PREROUTING (política ACCEPT)
alvo       prot opt source               destino

Chain POSTROUTING (política de DROP)
alvo       prot opt source               destino
MASQUERADE  todos    -  em qualquer lugar      alvo           em qualquer lugar
                                                    pr
Chain OUTPUT (política ACCEPT)                  ot opt source
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`destino` MASQUERADE

Mais uma vez, as regras de máscaras aparecem com uma meta de `MASQUERADE`.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Definir parâmetros de tempo para a IP Masquerade

Quando cada nova conexão é estabelecida, o software IP masquerade cria uma associação na memória entre cada um dos hosts envolvidos na conexão. Você pode ver essas associações a qualquer momento, olhando para o */ Proc / ip_masquerade / net* arquivo. Estas associações tempo de espera após um período de inatividade, no entanto.

Você pode definir o tempo limite de valores usando o `ipfwadm` comando. A sintaxe geral para isto é:

`<Ipfwadm-M-s`*tcp*`<>`*tcpfin*`<>`*udp*`>`

e para a `ipchains` comando é:

`ipchains-M-S <`*tcp*`<>`*tcpfin*`<>`*udp*`>`

A *iptables* implementação usa temporizadores padrão muito mais tempo e não permitem que você definir.

Cada um desses valores representa um timer usado pelo software de IP e de máscaras estão em unidades de segundos. A seguinte tabela resume os temporizadores e os seus significados:

Nome	Descrição
tcp	TCP timeout da sessão. Quanto tempo uma conexão TCP pode permanecer inativa antes da associação para que é removido.
tcpfin	TCP timeout após FIN. Quanto tempo uma associação continuará a ser depois de uma conexão TCP foi desconectado.
udp	UDP timeout da sessão. Quanto tempo uma conexão UDP pode permanecer inativa antes da associação para que é removido.

Server manipulação Pesquisas Nome

Manipulação de pesquisas de nome de domínio do servidor do hosts na LAN com mascaramento de IP sempre apresentou um problema. Há duas maneiras de acomodar o DNS em um ambiente de máscaras. Você pode dizer a cada um dos hosts que utilizam o DNS mesmo que a máquina roteador Linux faz, e deixar mascarado IP fazer a sua magia em sua solicitações de DNS. Alternativamente, você pode executar um servidor de nomes em cache na máquina Linux e ter cada um dos hosts na LAN usar a máquina Linux como seu DNS. Embora uma ação mais agressiva, esta é provavelmente a melhor opção, pois reduz o volume de tráfego DNS viajando na ligação à Internet e será marginalmente mais rápido para a maioria dos pedidos, uma vez que vai ser servido a partir do cache. A desvantagem desta configuração é que ela é mais complexa. "Cache-configuração apenas com o nome" no Capítulo 6 descreve como configurar um nome de cache servidor.

Mais Sobre Network Address Translation

A *netfilter* O software é capaz de muitos tipos diferentes de Network Address Translation. Masquerade IP é um simples aplicação da mesma.

É possível, por exemplo, para criar regras de NAT, que se traduzem apenas para determinados endereços ou intervalos de endereços e deixe intocados todos os outros, ou para converter endereços em pools de endereços ao invés de apenas um único endereço, como mascarada faz. Você pode, de facto, utilizar o `iptables` comando para gerar regras NAT que mapeiam praticamente qualquer-coisa, com combinações de jogos usando qualquer um dos atributos padrão, tais como endereço de origem, destino endereço, tipo de protocolo, número de porta, etc

Traduzindo o endereço de origem de um datagrama é conhecido como "NAT Source", ou SNAT, No *netfilter* documen-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

ção. Traduzindo o endereço de destino de um datagrama é conhecido como "Destination NAT", ou DNAT. Traduzindo

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

a porta TCP ou UDP é conhecido pelo termo `REDIRECT`.`SNAT`,`DNAT`E `REDIRECT` são alvos que você pode uso com o `iptables` comando para criar regras mais complexas e sofisticadas.

O tema da Network Address Translation e garante seus usos, pelo menos, um capítulo inteiro de seu próprio.[68] ONUfortu- Infelizmente não temos o espaço neste livro para cobri-lo em qualquer profundidade. Você deve ler o iptables-HOWTO para mais informações, se você estiver interessado em descobrir mais sobre como você pode usar rede Ad- vestido de tradução.

68 ... e talvez mesmo um livro inteiro!

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 12 - Características importantes da rede

Após o sucesso na criação de IP e resolver, então você deve olhar para os serviços que pretende oferecer ao longo dos rede. Este capítulo cobre a configuração de algumas aplicações de rede simples, incluindo o `inetd` servidor e os programas do `rlogin` da família. Também vamos abordar brevemente com o Remote Procedure Call inter- cara, sobre o qual serviços como o Network File System (NFS) eo Network Information System (NIS) são base. A configuração do NFS e NIS, porém, é mais complexa e são descritos em capítulos separados, como são o correio electrónico e novidades da rede.

Claro, não podemos cobrir todas as aplicações de rede neste livro. Se você quiser instalar um que não é discutido aqui, como `Discussão`,`gopher`Ou `http`, Por favor consulte as páginas de manual do servidor para maiores detalhes.

O inetd Super Server

Programas que oferecem serviços de aplicações através da rede são chamados de rede *daemons*. Um daemon é um programa que abre uma porta, mais uma porta de serviço bem conhecida, e aguarda conexões de entrada nele. Se um ocorre, o servidor cria um processo filho que aceita a conexão, enquanto o pai continua a ouvir novos pedidos. Este mecanismo funciona bem, mas tem algumas desvantagens, pelo menos uma instância de cada possível serviço que você deseja fornecer deve estar ativo na memória todos os momentos. Além disso, as rotinas de software que fazem o Acesse e movimentação portuária deve ser replicada em cada daemon de rede.

Para superar estas deficiências, a maioria das instalações Unix executar um daemon de rede especial, que você pode con- considerar uma "super servidor". Este daemon cria tomadas em nome de uma série de serviços e atende em todos eles simultaneamente. Quando uma ligação é recebida em qualquer uma dessas bases, o servidor aceita a super ligação e gera o servidor especificado para esta porta, passando o soquete para a criança através de gerir. A servidor retorna à escuta.

O servidor mais comum é chamada de super `inetd`, Daemon Internet. É iniciado no tempo de inicialização do sistema e tem A lista de serviços é administrar a partir de um arquivo de inicialização chamado */ Etc / inetd.conf*. Além desses servidores, há uma série de serviços realizados por trivial `inetd` próprio chamado *serviços internos*. Eles incluem `chargen`, Que simplesmente gera uma seqüência de caracteres, e `dia`, Que retorna a idéia do sistema da hora do dia.

Uma entrada neste arquivo é composto de uma única linha composta dos seguintes campos:

protocolo tipo de serviço esperar cmdline servidor usuário

Cada um dos campos é descrito na lista a seguir:

serviço

> Dá o nome do serviço. O nome do serviço tem de ser traduzido para um número de porta, olhando-o no */ Etc / services* arquivo. Este arquivo será descrito mais tarde neste capítulo na seção "Serviços e Proto- cols Files ".

tipo

> Especifica um tipo de socket, ou *stream* (Para protocolos orientados à conexão) ou *dgram* (Para o proto-datagrama cols). serviços baseados em TCP deve, portanto, use sempre *stream*, Enquanto os serviços baseados em UDP deve sempre uso *dgram*.

protocolo

> Nomes do protocolo de transporte utilizado pelo serviço. Este deve ser um nome de protocolo válido encontrado no *pró-* *colos* arquivo, explicou mais tarde.

esperar

> Esta opção só se aplica aos *dgram* soquetes. Ele pode ser *esperar* ou *nowait*. Se *esperar* é especificado, `inetd` executa apenas um servidor para a porta especificada a qualquer momento. Caso contrário, ele imediatamente continua a ouvir na porta após a execução do servidor.
>
> Isso é útil para "single-threaded" servidores que ler todos os datagramas de entrada até que não mais chegam, e em seguida, sair. A maioria dos servidores RPC são deste tipo, pelo que deve especificar *esperar*. O tipo oposto,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

"Multi-threaded" servidores, permitir que um número ilimitado de instâncias para executar simultaneamente. Esses servidores
deve especificar *nowait*.

usuário *stream* soquetes deve sempre usar *nowait*.

Este é o ID de login do usuário que será o dono do processo quando ele é executado. Esse será freqüentemente o *root* usuário, mas alguns serviços podem usar contas diferentes. É uma idéia muito boa para aplicar o princípio do menor privilégio aqui, que diz que você não deve executar um comando em uma conta privilegiada, se o programa não exige isso para o funcionamento adequado. Por exemplo, o servidor de notícias NNTP é executado como *servidor notícias*,
enquanto os serviços que podem representar um risco de segurança (tais como `tftp` ou `dedo`) São frequentemente executados como *ninguém*.

cmdline

Dá o caminho completo do programa de servidor para ser executado. serviços internos são marcados pela chave palavra *interna*.

Esta é a linha de comando a serem passados para o servidor. Ela começa com o nome do servidor para ser executado e pode incluir quaisquer argumentos que precisam ser passados para ele. Se você estiver usando o wrapper TCP, que espe-
verificam o caminho completo para o servidor aqui. Se não, então você apenas especificar o nome do servidor que você gostaria que ele
aparecem em uma lista de processos. Vamos falar sobre o TCP Wrapper em breve.

Este campo é vazio para serviços internos.

Uma amostra de *inetd.conf* arquivo é mostrado em Exemplo 12.1.A `dedo` serviço é comentada de modo que não está discapaz. Isso é feito muitas vezes por razões de segurança, porque ela pode ser usada por hackers para obter os nomes e outros detalhes
de usuários em seu sistema.

Exemplo 12.1: Exemplo de / etc / inetd.conf Arquivo

```
#
# Serviços inetd
ftp      stream tcp nowait root  / Usr / sbin /    l-in.ftpd
         ftpd
telnet   stream tcp nowait root  / Usr / sbin / -b/etc/issue telnetd in.telnetd
# Finger stream tcp nowait bin   / Usr / sbin / fingerd in.fingerd
# Tftp   dgram  udp esperar                        ninguém usr / sbin / tftpd
# Tftp           in.tftpd
         dgram  udp esperar                        ninguém usr / sbin / tftpd
                in.tftpd / boot / diskless
# Login  stream tcp nowait root  / Usr / sbin / in.rlogind rlogind
# Shell  stream tcp nowait root  / Usr / sbin /    in.rshd
rshd
# Exec   stream tcp nowait root  / Usr / sbin / rexecd  in.rexecd
#
#       inetd serviços internos
#
dia      stream tcp nowait root interna
dia      dgram  nowait root udp interna
tempo    stream tcp nowait root interna
tempo    dgram  nowait root udp interna
echo     stream tcp nowait root interna
echo     dgram  nowait root udp interna
descartar   stream tcp nowait root interna
descartar dgram  nowait root udp interna
chargen  stream tcp nowait root interna
chargen  dgram  nowait root udp interna
```

A `tftp` daemon é mostrado comentado também. `tftp` implementa o *Trivial File Transfer Protocol* (TFTP), que permite a alguém para transferir os arquivos de leitura de seu sistema sem verificar a senha
arg. Isso é especialmente prejudicial ao */ Etc / passwd* arquivo e, ainda mais quando você não tem uma passa-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

as palavras.

TFTP é normalmente utilizado por clientes diskless e XTerminals para baixar o seu código a partir de um servidor de boot. Se

você
necessidade de executar `tftpd` por essa razão, certifique-se de limitar o seu âmbito aos diretórios a partir do qual os clientes irão re-
trieve arquivos, você precisará adicionar os nomes de diretório para `tftpd`"Linha de comando do. Isso é mostrado no segundo `tftp` linha no exemplo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O tcpd Access Control Facility

Desde a abertura de um computador para acessar a rede envolve muitos riscos de segurança, os aplicativos

são projetados para proteger
contra vários tipos de ataques. Algumas características de segurança, entretanto, pode ser falho (mais drasticamente demonstrado pelo worm Internet RTM, que explorava um buraco em uma série de programas, incluindo as versões antigas do daemon sendmail mail), ou não fazem distinção entre hosts seguros de que os pedidos de um determinado serviço serão aceitas e insegura hosts cujos pedidos devem ser rejeitados. Nós já brevemente discutido o `finger` e `tftp` serviços. Administrador de Rede iria querer limitar o acesso a esses serviços "hosts confiáveis" apenas, o que é impossível com a configuração usual, para o qual `inetd` oferece este serviço, quer para todos os clientes ou não em tudo.

Uma ferramenta útil para gerenciar o acesso específica do host é `tcpd`, Muitas vezes chamado de daemon "wrapper".[69] Para os

serviços TCP
que você deseja monitorar ou proteger, ele é chamado em vez do programa servidor. `tcpd` verifica se o host remoto está permissão para usar esse serviço, e somente se isto for bem sucedido irá executar o programa servidor real. `tcpd` também registra o
pedido para o `syslog` daemon. Note que isso não funciona com serviços baseados em UDP.

Por exemplo, para envolver o `dedo` daemon, você tem que mudar a linha correspondente no *inetd.conf* a partir desta:

```
# Desembrulhou daemon de finger
dedo      stream tcp nowait bin    / Usr / sbin / fingerd in.fingerd
```

para isso:

```
# Finger daemon
envoltório              nowait  root    / Usr / sbin / tcpd     in.fingerd
dedo    stream  tcp
```

Sem adição de qualquer controle de acesso, isso vai aparecer para o cliente como o habitual `dedo` instalação, exceto que

qualquer
pedidos são registrados `syslog`'S *auth* facilidade.

Dois arquivos chamados */ Etc / hosts.allow* e */ Etc / hosts.deny* implementar controle de acesso. Eles contêm entradas que

permitem
e negar o acesso a determinados serviços e hosts. Quando `tcpd` lida com um pedido de um serviço como o `dedo` a partir de um host cliente chamado *biff.foobar.com*, Ele verifica *hosts.allow* e *hosts.deny* (Nesta ordem) para uma entrada correspondente ambos
o host de serviço e cliente. Se uma entrada for encontrada em *hosts.allow*, O acesso é concedido e `tcpd` não contoriamente o *hosts.deny* arquivo. Se nenhuma correspondência é encontrada na *hosts.allow* arquivo, mas uma correspondência for encontrada em *hosts.deny*, O re-
busca é rejeitada pelo encerramento da conexão. O pedido é aceite se nenhuma correspondência for encontrada.

Entradas nos arquivos de acesso parecido com este:

servicelist`:` *hostlist* `[:`*shellcmd*`]`

servicelist é uma lista de nomes de serviço de */ Etc / services*, Ou a palavra-chave *ALL*. Para corresponder a todos os serviços,

exceto `finger` e `tftp`, Use *ALL EXCETO* `dedo, tftp`.

hostlist é uma lista de nomes de máquinas, endereços IP, ou as palavras-chave *ALL*,*LOCAL*,*DESCONHECIDO* ou

PARANOID.ALL
corresponde a qualquer host, enquanto *LOCAL* hostnames correspondências que não contêm um ponto.[70]*DESCONHECIDO* corresponde a qualquer hosts
cujo nome ou endereço de pesquisa falhou. *PARANOID* corresponde a qualquer host cujo hostname não resolve voltar para seu endereço IP.[71] Um nome que começa com um ponto corresponde a todos os hosts cujo domínio é igual a este nome. Por exemplo,
. Foobar.com jogos *biff.foobar.com*, Mas não *nurks.fredsville.com*. Um padrão que termina com um ponto corresponde a qualquer host cujo endereço IP começa com o padrão fornecido, de modo *172.16.* jogos *172.16.32.0*, Mas não *172.15.9.1*. A padrão do formulário *n.n.n.n/m.m.m.m* é tratado como um endereço IP e máscara de rede, para que pudéssemos especificar nosso
exemplo padrão de forma como *172.16.0.0/255.255.0.0* em vez disso. Por último, qualquer padrão começando com um caractere "/"

PDF Creator PDF4Free v2.0 http://www.pdf4free.com

permite
você especifique um arquivo que se presume conter uma lista de padrões de nome ou endereço IP, um dos quais são allowed a combinar. Então, um padrão que parecia */ Var / acesso / TrustedHosts* faria com que o `tcpd` daemon ler que
arquivo, testar se qualquer uma das linhas em que combinava com o host de conexão.

Para negar o acesso à `dedo` e `tftp` serviços a todos, mas os anfitriões locais, colocando em */ Etc / hosts.deny*
e deixar */ Etc / hosts.allow* vazio:

```
in.tftpd, in.fingerd: ALL EXCEPT LOCAL, .Your.domain
```

69 Escrito por Wietse Venema, wietse@wzv.win.tue.nl.
70 hostnames Normalmente só local obtidos em pesquisas */ Etc / hosts* não contêm pontos.
71 Enquanto o nome sugere, é uma medida extrema, o *PARANOID* palavra-chave é um bom padrão, uma vez que protege contra as hostes malicioso fingindo ser alguém que eles não são. Nem todos os `tcpd` são fornecidos com *PARANOID* compilados, se o seu não é, você precisa recompilar `tcpd` usá-lo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O opcional *shellcmd* campo pode conter um comando a ser invocado quando a entrada é correspondido. Esta é a utilização ful criar armadilhas que podem expor potenciais agressores. O exemplo a seguir cria um arquivo de log lista o usuário e de acolhimento de ligação, e se o host não é vlager.vbrew.com ele irá acrescentar a saída de um `dedo` para esse host:

```
in.ftpd:. ALL EXCEPT LOCAL, vbrew.com: \
      echo "pedido de% d @ h%:>> / var / log / finger.log; \
      if [% h = "vlager.vbrew.com:"], então \
          l dedo @% h>> / var / log / finger.log \
      fi
```

A *% h* e *% D* argumentos são expandidos por `tcpd` para o nome da máquina cliente e nome do serviço, respectivamente. Por favor
referem-se ao *hosts_access (5)* página de manual para detalhes.

O Serviço de Protocolos e Arquivos

Os números de porta na qual certos "padrão" serviços são oferecidos são definidos no RFC Assigned Numbers.
Para permitir que os programas cliente e servidor para converter nomes de serviço a estes números, pelo menos parte da lista é mantida em
cada host, que é armazenado em um arquivo chamado */ Etc / services*. Uma entrada é composta da seguinte forma:

porta de serviço / protocolo [*aliases*]

Aqui, *serviço* especifica o nome do serviço, *porto* define a porta do serviço é oferecido, e *protocolo* define qual protocolo de transporte é utilizado. Comumente, o último campo seja *udp* ou *tcp*. É possível para um serviço a ser oferecidos para mais de um protocolo, bem como oferecer diferentes serviços na mesma porta, desde que o protocols são diferentes. A *aliases* campo permite especificar nomes alternativos para o mesmo serviço.

Normalmente, você não tem que alterar o arquivo de serviços que vem junto com o software de rede em seu Linux do sistema. No entanto, damos um pequeno trecho desse arquivo em Exemplo 12.2.

Exemplo 12.2: Exemplo de / etc / services Arquivo

```
# O arquivo de serviços:
#
# Serviços bem conhecidos
echo            7/tcp                   # Echo
echo            7/udp                   #
descartar       9/tcp  pia nula         # Descarte
descartar       9/udp  pia nula         #
dia            13/tcp                   # Diurno
dia            13/udp                   #
chargen        19/tcp  fonte ttytst     # Gerador de caracteres
chargen        19/udp  fonte ttytst     #
ftp-data       20/tcp                   # File Transfer Protocol (Dados)
ftp            21/tcp                   # File Transfer Protocol (Control)
telnet         23/tcp                   # Protocolo de Terminal Virtual
smtp           25/tcp                   # Simple Mail Transfer Protocol
nntp          119/tcp  readnews         # Network News Transfer Protocol
#
# Serviços UNIX
exec          512/tcp                   # BSD rexecd
golpe         512/udp  comsat           # Notificação por correio
login         Assíncronos 513/tcp       # Login remoto
que           513/udp  whod             # Afastadas e uptime
shell         514/tcp  cmd              # Comando remoto, não passwd usado
syslog        514/udp                   # Sistema remoto de log
impressora    515/tcp  spooler          # Spool de impressão remota
rota          520/udp  roteador roteados    # Protocolo de roteamento de informações
```

Note-se que o `echo` serviço é oferecido em sete porta para TCP e UDP, e que a porta 512 é usada para dois diferent serviços: execução remota (`rexec`) Usando TCP, eo `COMSAT` daemon, que notifica os usuários sobre novas mensagens, sobre UDP (ver `xbiff (1x)`).

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Como o arquivo de serviços, a biblioteca de rede precisa de uma maneira de traduzir os nomes de protocolos - por exemplo, aqueles utilizados
no arquivo de serviços - para os números de protocolo compreendido pela camada IP em outros hospedeiros. Isso é feito olhando para cima
o nome na */ Etc / protocols* arquivo. Ele contém uma entrada por linha, cada um contendo um nome de protocolo, e as associados número. Tendo a tocar esse arquivo é ainda mais improvável do que ter que mexer com */ Etc / services*. A samplo arquivo é dado em Exemplo de 12,3.

Exemplo 12.3: Um Exemplo de / etc / protocols Arquivo

```
#
# Internet (IP), protocolos
#
ip      0       IP              # Internet número do protocolo protocolo, pseudo
icmp    1       ICMP            # Internet Control Message Protocol
igmp    2       IGMP            # Internet protocol grupo multicast
tcp     6       TCP             # Transmission Control Protocol
udp     17      UDP             # User Datagram Protocol
-primas 255     RAW             # RAW interface IP
```

Chamada de procedimento remoto

O mecanismo geral para aplicações cliente-servidor é fornecido pelo *Chamada de procedimento remoto* (RPC) do pacote.
RPC foi desenvolvido pela Sun Microsystems e é uma coleção de ferramentas e funções de biblioteca. aplicações importantes, ções construídas em cima da RPC são o NIS, o Network Information System (descrito no Capítulo 13, *A Rede Informação do Sistema*) E NFS, Network File System (descrito no Capítulo 14, *O Network File System*),
que são descritas neste livro.

Um servidor RPC é composto por um conjunto de procedimentos que um cliente pode chamar através do envio de uma

solicitação de RPC ao
servidor, juntamente com os parâmetros de procedimento. O servidor irá invocar o procedimento indicado em nome da cliente, devolvendo o valor de retorno, se houver. Para ser independente da máquina, todos os dados trocados
entre cliente e servidor é convertido para o *Representação de Dados Externos* formato (XDR) pelo remetente, e
convertidas de volta para a representação local da máquina pelo receptor. RPC se baseia em UDP padrão e meia-TCP ets para o transporte de XDR dados formatados para o host remoto. A Sun tem graciosamente colocado RPC no domínio público;
é descrito em uma série de RFCs.

Às vezes, as melhorias para um aplicativo RPC introduzir alterações de incompatibilidade na interface chamada de

procedimento.
É claro, basta mudar o servidor iria falhar todos os aplicativos que ainda esperam o comportamento original. Há-
Portanto, programas de RPC tem números de versão que lhes é atribuído, geralmente começando com 1 e com cada nova versão da interface RPC, este contador será colidido acima. Muitas vezes, um servidor pode oferecer várias versões em simultâneo; clientes, então, indicar pelo número de versão nos seus pedidos de que a execução do serviço que eles querem
uso.

A comunicação entre clientes e servidores RPC é um tanto peculiar. Um servidor RPC oferece uma ou mais
coleções de procedimentos; cada conjunto é chamado de *programa* e é identificado exclusivamente por um *número de programa*. Uma lista
que mapeia os nomes de serviço para os números do programa geralmente é mantido em */ Etc / rpc*, Um trecho do que é mostrado na
Exemplo de 12,4.

Exemplo 12.4: Uma amostra do arquivo / etc / rpc

```
#
# / Etc / rpc - diversos serviços baseados em RPC
#
portmapper              ypbind
rstatd                  walld
rusersd                 yppasswdd
nfs                     bootparam
ypserv                  ypupdated
mountd
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
100000  portmap sunrpc100005  montagem showmount
100001  perfmeter rup 100007
RStat rstat_svc       100008  desligamento rwall
100002  rusers        100009  yppasswd
100003  nfsprog       100026
100004  ypprog        100028  ypupdate
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Em redes TCP / IP, os autores da RPC enfrentou o problema de números de programa de mapeamento de rede genérica serviços. Eles projetaram cada servidor para fornecer uma conexão TCP e uma porta UDP para cada programa e cada versão. Geralmente, os aplicativos RPC usar UDP ao enviar dados, e cair para TCP somente quando os dados a serem transridos não caber em um único datagrama UDP.

Naturalmente, os programas cliente precisa saber a que porta um número de programa de mapas. Usando um arquivo de

configuração para
isso seria demasiado inflexíveis, desde aplicativos de RPC não usam portas reservadas, não há nenhuma garantia que uma porta originalmente concebido para ser usado pelo nosso aplicativo de banco de dados não tenha sido tomada por algum outro processo. Portanto, RPC
aplicações de escolher qualquer porta que podem começar e registrá-lo com um programa especial chamado *daemon portmapper*. A
atos portmapper como um agente de serviços para todos os servidores RPC rodando em sua máquina. Um cliente que deseja um contato
serviço com um número determinado programa primeiro consulta o portmapper no host do servidor, que retorna o TCP e números de porta UDP que o serviço possa ser alcançado em.

Este método introduz um ponto único de falha, muito parecido com o `inetd` daemon faz para o padrão de Berkeley serviços. No entanto, neste caso, é até um pouco pior, porque quando o portmapper morre, todas as informações de porta RPC é perdido, isso normalmente significa que você tem que reiniciar todos os servidores RPC manualmente ou reiniciar a máquina inteira.

No Linux, o portmapper é chamado */ Sbin / portmap*, Ou às vezes */ Usr / sbin / rpc.portmap*. Para além de fazer certo é iniciado a partir de seus scripts de inicialização de rede, o portmapper não requer qualquer configuração.

Configurando o login remoto e Execução

Muitas vezes é muito útil para executar um comando em um host remoto e têm entrada ou saída deste comando ser lidos ou escritos, uma conexão de rede.

Os comandos tradicionais utilizados para executar comandos em máquinas remotas são `rlogin`,`rsh` e `rcp`. Vimos um exemplo da `rlogin` comando no Capítulo 1, *Introdução às Redes* na seção "Introdução ao Redes TCP / IP ". Nós brevemente discutidas as questões de segurança associadas a ele de" Sistema de Segurança "e sugesugerido `ssh` como um substituto. A `ssh` pacote fornece substitutos chamados `slogin`,`ssh`E `scp`.

Cada um destes comandos gera um shell na máquina remota e permite ao usuário executar comandos. Claro, o cliente precisa ter uma conta na máquina remota, onde o comando será executado. Assim, todos esses comandos usam um processo de autenticação. A *r* comandos usam um nome de usuário simples e troca de senha serentre os hosts sem criptografia, para ouvir qualquer um poderia interceptar facilmente as senhas. A `ssh` comando Suite oferece um alto nível de segurança: ele usa uma técnica chamada `Criptografia de chave pública`, Que fornece autenticação e criptografia entre os hosts para garantir que nem senhas nem dados são sessão facilmente interceptadas por outras máquinas.

É possível simplificar os controlos de autenticação para determinados usuários ainda mais. Por exemplo, se você freqüentemente

tem que
entrar em outras máquinas na sua rede, você pode querer ser admitido sem ter que digitar a sua senha o tempo todo. Isso sempre foi possível com a *r* comandos, mas o `ssh` suite permite que você faça isso um pouco mais facilmente. Ainda não é uma grande idéia, porque significa que se uma conta em uma máquina é rompida, o acesso pode ser adquirida para todas as outras contas que o usuário tenha configurado para logon sem senha, mas é muito conveniente e pessoas vai usá-lo.

Vamos falar sobre como remover o *r* comandos e recebendo `ssh` para trabalhar em seu lugar.

Desativar o `r`; Comandos

Comece por retirar o `r` comandos se eles estão instalados. A maneira mais fácil de desativar o antigo `r` comandos é comentar (ou remover) suas inscrições no */ Etc / inetd.conf* arquivo. As entradas relevantes será algo parecido com isso:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# Shell, exec login, ea conversa é BSD protocolos.
shell    stream  tcp     nowait  root  / Usr / sbin / usr / tcpd / sbin / in.rshd
login    stream  tcp     nowait  root  / Usr / sbin / usr / tcpd / sbin / in.rlogind
exec     stream  tcp     nowait  root  / Usr / sbin / usr / tcpd / sbin / in.rexecd
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Você pode comentá-las, colocando um # personagem no começo de cada linha, ou excluir as linhas completamente. Lembre, você precisa reiniciar o `inetd` daemon para que esta alteração tenha efeito. Idealmente, você deve remover o daemon programas em si, também.

Instalando e Configurando ssh

OpenSSH é uma versão livre da suíte de programas de ssh, o porto Linux pode ser encontrada em http://violet.ibs.com.au/openssh/ umª na maioria das distribuições Linux modernas.[72] Não vamos descrever aqui a compilação; boas instruções estão incluídas na fonte. Se você pode instalá-lo de um pacote pré-compilado, então provavelmente é sensato fazê-lo.

Existem duas partes para uma `ssh` sessão. Há uma `ssh` cliente que você precisa para configurar e executar no local acolhimento e uma `ssh` daemon que deve estar em execução no host remoto.

O daemon ssh

A `sshd` daemon é o programa que monitora as conexões de rede `ssh` clientes, gerencia Authentication, e executa o comando solicitado. Tem um arquivo de configuração principal, chamado */ Etc / ssh / sshd_config* e um arquivo especial que contém uma chave usada pelo processo de autenticação e criptografia para representar o fim de acolhimento. Cada
host e cada cliente tem sua própria chave.

Um utilitário chamado `ssh-keygen` é fornecido para gerar uma chave aleatória. Isso geralmente é usado uma vez na instalação tempo para gerar a chave do anfitrião, que o administrador do sistema, geralmente, armazena em um arquivo chamado */ Etc / ssh_host_key / ssh*.
As chaves podem ser de qualquer comprimento de 512 bits ou superior. Por padrão, `ssh-keygen` gera chaves de 1024 bits em comprimento, ea maioria das pessoas utilizar o padrão. Para gerar uma chave aleatória, você poderia chamar o `ssh-keygen` com-
mando assim:

```
# ssh-keygen-f / etc / ssh / ssh_host_key
```

Você será solicitado a digitar uma senha. No entanto, as chaves de acolhimento não deve usar uma senha, então basta pressionar o
volte a chave para deixá-la em branco. A saída do programa será algo parecido com:

```
A geração de chaves RSA:      ..... Oooooo oooooo ..............................
A geração de chaves completo.
Enter passphrase (vazio para nenhum passphrase):
Entre no mesmo passphrase outra vez:
Sua identificação foi conservada em / etc / ssh / ssh_host_key
Sua chave pública foi gravada em / etc / ssh / ssh_host_key.pub
A impressão digital da chave é:
1024 3: 14:78:8 E: 5a: A3: 6b: bc: b0: 69:10:23: b7: d8: root @ 56:82 moria
```

Você vai descobrir no final que dois arquivos foram criados. A primeira é chamada de chave privada, que devem ser mantidos secreto e será em */ Etc / ssh_host_key / ssh*. A segunda é chamada de chave pública e é um que você pode compartilhar, mas estará em */ Etc / ssh_host_key.pub / ssh*.

Armado com as chaves para `ssh` comunicação, você precisa criar um arquivo de configuração. A `ssh` suite é muito arquivo de configuração poderosa e pode conter muitas opções. Vamos apresentar um exemplo simples para começar; você deve consultar o `ssh` documentação para permitir outras funcionalidades. O código a seguir mostra um cofre e minimal `sshd` arquivo de configuração. O resto das opções de configuração são detalhados no `sshd`(8) manpage:

```
# / Etc / ssh / sshd_config
#

# O IP adddresses para escutar as conexões por diante. 0.0.0.0, todas as
# Endereços locais.
ListenAddress 0.0.0.0

# A porta TCP para escutar as conexões. O padrão é 22.
Port 22

# O nome do arquivo de chave.
HostKey / etc / ssh_host_key / ssh
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

72 OpenSSH foi desenvolvido pelo projeto OpenBSD e é um bom exemplo dos benefícios do software livre.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# O comprimento da chave em bits.
ServerKeyBits 1024

# Será que devemos permitir logins via SSH?
PermitRootLogin no

# Se o diretório de usuários daemon ssh seleção em casa e permissões de arquivos?
# São seguros antes de permitir o login?
StrictModes sim

# Será que devemos permitir velho ~ /. Rhosts e / etc / hosts.equiv método de
autenticação?
RhostsAuthentication não
# Será que devemos permitir a autenticação RSA pura?
RSAAuthentication sim
# Será que devemos permitir que a autenticação de senha?
PasswordAuthentication sim

# Será que devemos permitir que / etc / hosts.equiv combinado com autenticação RSA de
acolhimento?
RhostsRSAAuthentication não
# Será que devemos ignorar ~ / arquivos. Rhosts?
IgnoreRhosts sim
# Será que devemos permitir logins para contas com senhas vazias?
PermitEmptyPasswords não
```

É importante certificar-se as permissões dos arquivos de configuração estão corretas para garantir a segurança do sistema é mantida. Use os seguintes comandos:

```
#  chown-R root: root / etc / ssh
#  chmod 755 / etc / ssh
#  chmod 600 / etc / ssh / ssh_host_key
#  chmod 644 / etc / ssh / ssh_host_key.pub
#  chmod 644 / etc / ssh / sshd_config
```

A fase final do `sshd` daemon de administração é executá-lo. Normalmente, você criar um *rc* arquivo para ele ou adicioná-la a um
já existente, para que ele seja executado automaticamente durante o boot. O daemon é executado autônomo e não requer qualquer entrada na */ Etc / inetd.conf* arquivo. O daemon deve ser executado como o `root` usuário. A sintaxe é muito simples:

```
/ Usr / sbin / sshd
```

A `sshd` daemon irá automaticamente colocar-se em segundo plano quando está sendo executado. Você agora está pronto para aceitar *ssh* conexões.

O cliente ssh

Há uma série de `ssh` programas de cliente: `slogin`,`scp` e `ssh`. Cada um lê a mesma configuração
arquivo, geralmente chamado */ Etc / ssh / ssh_config*. Cada um deles também ler arquivos de configuração do *. Ssh* diretório no diretório home do usuário que executa-los. O mais importante desses arquivos é o *.ssh / config* arquivo, que pode contém opções que substituem as especificadas na */ Etc / ssh / ssh_config* arquivo, o *.ssh / identity* arquivo, que contém própria chave privada do usuário, e os correspondentes *.ssh / identity.pub* arquivo, contendo a chave pública do usuário. Outras os arquivos são importantes *.ssh / known_hosts* e *.ssh / authorized_keys*, Falaremos sobre isso mais tarde em "Usando ssh".Em primeiro lugar,
vamos criar o arquivo de configuração global e os arquivos dos usuários-chave.

/ Etc / ssh / ssh_config é muito semelhante ao do arquivo de configuração do servidor. Novamente, existem muitos recursos que você pode con-
figura, mas uma configuração mínima se parece com aqueles apresentados no Exemplo de 12,5.O resto da configuração de opções são detalhados no `sshd (8)` manpage. Você pode adicionar seções que correspondem a máquinas específicas ou grupos de hosts.
O parâmetro para o "`Host`"A declaração pode ser o nome completo de um host ou uma especificação de curinga, como usamos em nosso exemplo, para combinar com todos os hosts. Poderíamos criar uma entrada utilizada, por exemplo, `Host *. Vbrew.com` para combinar com qualquer host na `vbrew.com` domínio.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Exemplo 12.5: Exemplo de arquivo de configuração do cliente ssh

```
# / Etc / ssh / ssh_config

# opções padrão para usar quando conectar com um host remoto
Host *
  # Comprimir os dados da sessão?
  Compressão sim
  # .. utilizando o nível de compressão? (1 - rápido / pobre, 9 - lento /
  bom)
  CompressionLevel 6

  # Queda de volta para rsh se a conexão segura falhar?
  FallBackToRsh não

  # Será que devemos enviar mensagens keep-alive? Útil se você usar
  máscaras IP
  KeepAlive yes

  # Tentar autenticação RSA?
  RSAAuthentication sim
  # Tentar autenticação RSA em combinação com. Rhosts?
  RhostsRSAAuthentication sim
```

Nós mencionamos na seção de configuração do servidor que cada host eo usuário tem uma chave. A chave do usuário é armazenado em
sua *~ / .ssh / Indentity* arquivo. Para gerar a chave, use o mesmo `ssh-keygen` comando como costumávamos geral-comeu a chave do anfitrião, só que desta vez você não precisa especificar o nome do arquivo no qual você salvar a chave. A `ssh-keygen` padrões para o local correto, mas ele pede que você digite um nome de arquivo no caso de você gostaria de guardá-lo
em outros lugares. Às vezes, é útil ter múltiplos arquivos de identidade, de modo `ssh` permite isso. Tal como antes, `ssh-keygen` solicitará a entrada de uma senha. Passphrases acrescentar ainda um outro nível de segurança e são um bom idéia. Sua senha não será exibida na tela quando você digitá-la.

AVISO: Não há maneira de recuperar uma senha se esquecê-la. Certifique-se que é algo que será re-membro, mas como com todas as senhas, fazer algo que não é óbvia, como um nome próprio ou o seu nome. Para um senha para ser verdadeiramente eficaz, deve ser entre 10 e 30 caracteres e não pode ser em prosa planície Inglês. Tente jogar alguns personagens incomuns. Se você esquecer sua senha, você será obrigado a gerar uma nova chave.

Você deve perguntar a cada um de seus usuários a executar o `ssh-keygen` comando apenas uma vez para garantir o seu arquivo de chave é cre-
ated corretamente. A `ssh-keygen` vai criar a sua *~ /. Ssh /* diretórios para eles com as devidas permissões e criar suas chaves privadas e público em *.ssh / identity* e *.ssh / identity.pub*, Respectivamente. Uma sessão de amostra deve algo parecido com:

```
$ ssh-keygen
A geração de chaves RSA:      ....... Oooooo ..............................
A geração de chaves completo.
Digite arquivo no qual deseja salvar a chave (/ home / maggie / .ssh / identity):
Enter passphrase (vazio para nenhum passphrase):
Entre no mesmo passphrase outra vez:
Sua identificação foi conservada em / home / maggie / .ssh / identity.
Sua chave pública foi gravada em / home / maggie / .ssh / identity.pub.
A impressão digital da chave é:
1024 85:49:53: f4: 8: D6: D9: 05: d0: 1F: 23: c4: D7: maggie @ 11:67 moria: 2a
$
```

Agora `ssh` está pronto para ser executado.

Usando ssh

Agora devemos ter a `ssh` comando e é associada programas instalados e prontos para rodar. Vamos agora dar uma rápida olhada em como executá-los.

Primeiro, vamos tentar um login remoto a um hospedeiro. Podemos usar o `slogin` programa em muito da mesma maneira como foi utilizado o

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`rlogin` programa, em nosso exemplo anterior no livro. A primeira vez que tentar uma conexão com um host, o `ssh` cliente irá recuperar a chave pública do host e pedir que você confirme sua identidade por avisar-lhe um curto Versão precisa da chave pública chamado `impressão digital`.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O administrador na máquina remota deve ter lhe fornecido previamente com sua impressão digital de chave pública, que você deve adicionar à sua *.ssh / known_hosts* arquivo. Se o administrador remoto não forneceu-lhe a adequada chave, você pode se conectar ao host remoto, mas `ssh` irá avisá-lo que ele tem uma chave e pedir-lhe se quiser aceitar o oferecido pelo host remoto. Assumindo que você está certo de que ninguém está envolvido em DNS falsificação e você está na verdade falando com o host correto, responder afirmativamente à solicitação. A chave relevantes é então armazenado
automaticamente em seu *.ssh / known_hosts* e você não será solicitado novamente. Se, em uma futura conexão tentativa, a chave pública recuperados a partir desse acolhimento não corresponde ao que é armazenado, você será avisado, seja-porque isso representa uma quebra de segurança potencial.

Um login pela primeira vez a um host remoto será algo parecido com:

```
$ vchianti.vbrew.com slogin
A autenticidade do "vchianti.vbrew.com 'host não pode ser estabelecida.
impressão digital da chave é de 1024 7b: d4: a8: 28: c5: 19:52:53:3 um: fe: 8D: 95:
dd: 14:93: F5.
Tem certeza que quer continuar a conectar (sim / não)? sim
Atenção: Permanentemente acrescentado »vchianti.vbrew.com, 172.16.2.3" na lista de /
    máquinas conhecidas.
maggie@vchianti.vbrew.com senha é:
Último login: Ter Fev   1 23:28:58 2000 de vstout.vbrew.com
$
```

Você será solicitado para uma senha, que você deve responder com a senha que pertencem à distância ac-contagem, não a um local. Essa senha não é exibida quando você digita.

Sem argumentos especiais, `slogin` tentará entrar com o mesmo ID de usuário utilizado na máquina local.

Você pode substituir isso usando o `-L` argumento, fornecendo um nome alternativo de login na máquina remota. Isto é o que fizemos em nosso exemplo anterior no livro.

Podemos copiar arquivos de e para o host remoto usando o `scp` programa. Sua sintaxe é semelhante ao convencional `cp` com a ressalva de que você pode especificar um hostname antes de um nome de arquivo, o que significa que o caminho do arquivo está no
host especificado. O exemplo a seguir ilustra `scp` sintaxe, copiando um arquivo local chamado */ Tmp / fred* ao */ Home maggie / /* do host remoto chianti.vbrew.com:

```
$ scp / tmp vchianti.vbrew.com / Fred: / home / maggie /
maggie@vchianti.vbrew.com senha é:
fred                  100% |*****************************| 50165   00:01 ETA
```

Mais uma vez, você será solicitado para uma senha. A `scp` comando exibe mensagens de andamento útil por padrão. Você pode copiar um arquivo de um host remoto com a mesma facilidade, basta especificar o nome do host e filepath como fonte e o caminho local como destino. É ainda possível copiar um arquivo de um host remoto para algum outro host remoto, mas é algo que você normalmente não quer fazer, porque todos os dados viajam através de seu anfitrião.

Você pode executar comandos em máquinas remotas usando o `ssh` comando. Novamente, sua sintaxe é muito simples. Vamos temos o nosso usuário maggie recuperar o diretório raiz do host remoto vchianti.vbrew.com. Ela ia fazer isso com:

```
$ ssh vchianti.vbrew.com ls-CF /
maggie@vchianti.vbrew.com senha é:
/ bin   console @ dos /    home /   lost + found /      @ pub / tmp     vmlinuz @
/ boot  / dev     etc /    / initrd mnt /        root / / usr vmlinuz.old @
/ cdrom disco /   disquete /  lib / proc /       sbin / var /
```

Você pode colocar `ssh` em uma tubulação de entrada de comando e tubo de programa / saída ou a partir dele, tal como qualquer outro com-
mando, exceto que a entrada ou saída é direcionada para ou a partir do host remoto via `ssh` conexão. Aqui está um exemplo de como você pode usar esse recurso em combinação com o `alcatrão` comando para copiar um diretório inteiro com subdiretórios e arquivos de um host remoto para o host local:

```
$ ssh vchianti.vbrew.com "tar cf - / etc / | tar xvf -
maggie@vchianti.vbrew.com senha é:
etc / GNUstep
etc / Muttrc
etc / Net
etc/X11
etc / adduser.conf
..
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Aqui estamos cercados o comando que será executado com aspas para deixar claro o que é passado como um argumento para `ssh` eo que é usado pelo shell local. Este comando executa o `alcatrão` comando do controle remoto host para arquivar o */ Etc /* diretório e escrever a saída para a saída padrão. Nós canalizada para uma instância do `alcatrão` comando em execução no nosso host local em extrair o modo de leitura da entrada padrão.

Mais uma vez, nós fomos alertados para a senha. Agora você pode ver porque é que a encorajou a configurar `ssh` de modo que ele não lhe pedir senhas o tempo todo! Vamos agora configurar o nosso local `ssh` cliente para que ele não será imediata uma senha ao se conectar ao *vchianti.vbrew.com* host. Nós mencionamos o *.ssh / authorized_keys* arquivo anterior, que é onde ele é usado. A *.ssh / authorized_keys* arquivo contém a *público* chaves em qualquer usuário remoto ac-Conta-se que queremos automaticamente login. Você pode configurar logins automáticos, copiando o conteúdo do *.ssh / identity.pub* da *remoto* conta em nosso local *.ssh / authorized_keys* arquivo. É vital que a permis-file ções do *.ssh / authorized_keys* permitir apenas que você leia e escreva, ninguém pode roubar e usar as teclas para entrar para a conta remota. Para garantir que as permissões estão corretas, a mudança *.ssh / authorized_keys*, Conforme mostrado:

```
$ chmod 600 ~ / .ssh / authorized_keys
```

As chaves públicas são uma longa *único* linha de texto simples. Se você usar o copiar e colar para duplicar a chave em seu local arquivo, certifique-se de remover quaisquer caracteres de fim de linha que poderia ter sido introduzidas ao longo do caminho. A *.ssh / authorized_keys* arquivo pode conter muitas chaves, cada um em uma linha própria.

A `ssh` conjunto de ferramentas é muito poderoso e há muitas outras características úteis e opções que será interessados em explorar. Por favor, consulte as páginas de manual e outra documentação que é fornecida com o pacote de idade para mais informações.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 13 - O Sistema de Informação de Rede

Quando você está correndo de uma rede de área local, o seu objectivo global é, geralmente, para proporcionar um ambiente para seus usuários
que torna a rede transparente. Um passo importante é manter os dados vitais, tais como conta de usuário no-
formação sincronizada entre todos os hosts. Isso proporciona aos usuários a liberdade de mudar de máquina para ma-
chine sem a inconveniência de ter que lembrar de senhas diferentes e copiar dados de uma máquina para
o outro. Os dados que são armazenados centralmente, não precisam ser replicados, desde que haja alguma forma conveniente de acessá-lo de um host conectado à rede. Ao armazenar informações administrativas importantes centralmente, você pode fazer assegurar a coerência dos dados, aumentar a flexibilidade para os usuários, permitindo-lhes passar de hospedeiro para host de forma transparente, e tornar a vida do administrador do sistema muito mais fácil manter uma única cópia do informações para manter, quando necessário.

Anteriormente discutimos um exemplo importante desse conceito que é utilizado na Internet - o Nome de Domínio System (DNS). DNS serve uma gama limitada de informação, o mais importante é o mapeamento entre host
nome e endereço IP. Para outros tipos de informações, não existe tal serviço especializado. Além disso, se você homem idade apenas uma pequena LAN sem conectividade com a Internet, configurar DNS pode não parecer valer a pena.

Isto é porque a Sun desenvolveu o *Rede de Sistema de Informação* (NIS). NEI fornece facilitar acesso genérico de banco de dados laços que podem ser usados para distribuir, por exemplo, informações contidas no *passwd* e *grupos* arquivos para todos os hosts em sua rede. Isso torna a rede aparece como um sistema único, com as mesmas contas em todos os hosts. Simi-
particularmente, você pode usar o NIS para distribuir as informações de host */ Etc / hosts* para todas as máquinas na rede.

NIS é baseado em RPC, e inclui um servidor, uma biblioteca do lado do cliente, e diversas ferramentas administrativas.

Originalmente,
NIS foi chamado *Páginas amarelas*, Ou AP, que ainda é usado para se referir a ele. Infelizmente, o nome é uma marca comercial da
British Telecom, que exigia a queda dom esse nome. Como as coisas vão, alguns nomes de ficar com as pessoas, e assim YP
vive como um prefixo para os nomes da maioria dos comandos NIS-relacionados, tais como `ypserv` e `ypbind`.

Hoje, o NIS está disponível para praticamente todos os Unixes, e existem implementações gratuitas. BSD Net-2 lançado um que tenha sido derivada de uma aplicação de domínio público de referência doados por dom. A biblioteca cliente código desta libertação foi no Linux *libc* por um longo tempo, e os programas administrativos foram portados para Linux pela Swen Th [Unhandled SDATA: [uuml]] mmler.[73] Um servidor NIS está faltando o im-referência mentação, no entanto.

Peter Eriksson desenvolveu uma nova aplicação chamada NYS.[74] Ele suporta tanto NIS simples e dom muito en-
Hanced NIS +. NYS não apenas fornece um conjunto de ferramentas de NIS e um servidor, mas também adiciona um novo conjunto de biblioteca
funções que precisam ser compiladas em seu *libc* se você quiser usá-lo. Isso inclui um regime de nova configuração para a resolução de nomes que substitui o actual regime de utilização *host.conf*.

A libc GNU, conhecido como *libc6* na comunidade Linux, inclui uma versão atualizada do NIS tradicional sup-
porto desenvolvido por Thorsten Kukuk.[75] Ele suporta todas as funções de biblioteca que NYS prestados e também usa a esquema de configuração avançada do NYS. Você ainda precisará das ferramentas e do servidor, mas a utilização do GNU *libc* poupa-lhe o
problema de ter que se meter com o patch e recompilar a biblioteca.

Este capítulo enfoca o apoio NIS incluídos no GNU *libc* vez que os outros dois pacotes. Se você fizer
deseja executar algum destes pacotes, as instruções neste capítulo podem ou não ser suficiente. Para complementar informações, consulte o NIS-HOWTO ou um livro como *Gerenciando NFS e NIS* por Hal Stern (O'Reilly).

Familiarizando-se com NIS

NIS mantém as informações do banco de dados em arquivos chamados *mapas*, Que contém pares chave-valor. Um exemplo de um valor de chave
par é o nome de login do usuário e da forma criptografada de sua senha de logon. Os mapas são armazenados em um sistema central
executando o servidor de NIS, a partir do qual os clientes podem recuperar as informações através de várias chamadas RPC. Muito fre-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Consequentemente, os mapas são armazenados em arquivos DBM.[76]

73 Swen pode ser alcançado em swen@uni-paderborn.de. Os clientes NIS estão disponíveis como *yp-linux.tar.gz* a partir de *metalab.unc.edu* em *sis-TEM / Rede*.

74 Pedro pode ser alcançado em pen@lysator.liu.se. A versão atual do NYS é 1.2.8.

75 Thorsten pode ser atingido com kukuk@uni-paderborn.de.

76 DBM é uma biblioteca simples de gerenciamento de banco de dados que usa técnicas de hashing para acelerar as operações de busca. Há uma execução DBM livre implementação do projeto GNU chamado *gdbm*, Que faz parte da maioria das distribuições Linux.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Os mapas em si são normalmente gerados a partir de arquivos de texto mestre como */ Etc / hosts* ou */ Etc / passwd*. Para alguns imagens, vários mapas são criados, um para cada tipo de chave de busca. Por exemplo, você pode procurar o *hosts* arquivo para um hostname, bem como para um endereço IP. Assim, dois mapas NIS são derivados a partir dele, chamado *hosts.byname* e *hosts.byaddr*.Tabela 13.1 listas mapas comuns e os ficheiros a partir do qual eles são gerados.

Tabela 13.1: Alguns mapas NIS padrão e os arquivos correspondentes

Master File	Mapa (s)	Descrição
/ Etc / hosts	*hosts.byname,hosts.byaddr*	Mapeia endereços IP para nomes de host
/ Etc / networks	*networks.byname,networks.byaddr*	Mapas de rede endereços IP para nomes de rede
/ Etc / passwd	*passwd.byname,passwd.byuid*	Mapas senhas criptografadas para nomes de login do usuário
/ Etc / group	*group.byname,group.bygid*	Mapas Grupo IDs para nomes de grupo
/ Etc / services	*services.byname,services.bynumber*	descrições de serviço Maps para serviços de nomes
/ Etc / rpc	*rpc.byname,rpc.bynumber*	Mapas Sun RPC números de serviço para serviço RPC nomes
/ Etc / protocols	*protocols.byname,protocols.bynumber*	os números de protocolo Maps para nomes de protocolos
/ Usr / lib / aliases	*mail.aliases*	aliases mail Maps para enviar nomes de alias

Você pode encontrar suporte para outros arquivos e mapas em outros pacotes NIS. Estes geralmente contêm informações para aplicações que não foram discutidos neste livro, como o *bootparams* mapa que é utilizado por Sun `bootparamd` servidor.

Para alguns mapas, as pessoas geralmente usam *apelidos*, Que são mais curtos e, portanto, mais fácil de digitar. Note que estes apelidos só são compreendidas pela `ypcat` e `ypmatch`, Duas ferramentas para verificar a configuração do NIS. Para obter uma lista completa dos apelidos entendida por estas ferramentas, execute o seguinte comando:

```
$ ypcat-x
Use "passwd" para "passwd.byname"
Use "grupo" para "group.byname"
Use "redes" para "networks.byaddr"
Use "hosts" para "hosts.byaddr"
Use "protocolos" para "protocols.bynumber"
Use "serviços" para "services.byname"
Use "apelidos" para "mail.aliases"
Use "ethers" para "ethers.byname"
```

O programa servidor NIS é tradicionalmente chamado `ypserv`. Para uma rede de média, um único servidor, geralmente é suficiente; grandes redes pode optar por executar vários destes em máquinas diferentes e diferentes segmentos da rede para aliviar a carga sobre o servidor de máquinas e roteadores. Esses servidores estão sincronizados, fazendo um deles o *servidor mestre*, E os outros *servidores escravos*. Os mapas são criados somente no host do servidor mestre. A partir daí, eles são distribuídos a todos os escravos.

Temos vindo a falar muito vagamente sobre "redes". Há um termo distintivo NIS que se refere a uma coleção de todos os hosts que compartilhar parte de seus dados de configuração do sistema através da NEI: *domínio NIS*. Infelizmente, NIS domínios não têm absolutamente nada em comum com os domínios que encontramos no DNS. Para evitar qualquer ambiguidade ao longo deste capítulo, portanto, sempre especificar qual tipo de domínio que queremos dizer.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

domínios NIS têm uma função puramente administrativa. Elas são invisíveis aos usuários, exceto para a partilha de senhas entre todas as máquinas no domínio. Portanto, o nome dado a um domínio NIS é relevante apenas para administradores. Normalmente, qualquer nome serve, contanto que ele é diferente de qualquer outro nome de domínio NIS em seu
rede local. Por exemplo, o administrador na Cervejaria Virtual pode optar por criar dois domínios NIS, um para a mesma fábrica, e um para a Adega, que ela nomes *cervejaria* e *vinícola* , respectivamente. Outro bastante regime comum é simplesmente usar o nome de domínio DNS para NIS também.

Para definir e exibir o nome de domínio NIS do seu host, você pode usar o `domainname` comando. Quando invocado sem nenhum argumento, ele imprime o nome do domínio atual NIS; para definir o nome de domínio, você deve se tornar o superusuário:

```
# cervejaria domainname
```

domínios NIS determinar qual servidor NIS um aplicativo de consulta. Por exemplo, o `login` programa em um host na adega deve, naturalmente, consulta apenas a Adega do servidor NIS (ou um deles, se houver várias) para um informações de usuário, senha enquanto um aplicativo em um host Cervejaria deve ficar com o servidor da cervejaria.

Um mistério agora continua a ser resolvido: como é que um cliente saber em qual servidor se conectar? O mais simples abordagem seria utilizar um arquivo de configuração que os nomes de acolhimento em que se encontrar o servidor. No entanto, esta abordagem
é bastante inflexível, pois não permitem que os clientes usam servidores diferentes (do mesmo domínio, é claro) dependendo de sua disponibilidade. Portanto, as implementações de NIS contar com um daemon chamado especial `ypbind` para
detectar um servidor NIS adequados em seu domínio NIS. Antes de realizar qualquer consulta NIS, um primeiro pedido encontra fora do `ypbind` que servidor usar.

`ypbind` sondas para servidores de radiodifusão com a rede IP local, o primeiro a responder será considerado o mais rápido e é usado em todas as consultas subseqüentes NIS. Após um determinado intervalo de tempo decorrido, ou se o servidor ser-
vem disponível, `ypbind` sondas para servidores ativos novamente.

Ligação dinâmica é útil apenas quando a rede oferece mais de um servidor NIS. Ligação dinâmica também introduz um problema de segurança. `ypbind` acredita cegamente em quem quer respostas, quer se trate de um servidor NIS humilde ou
um invasor mal-intencionado. Desnecessário dizer, isso se torna especialmente problemático se você gerenciar seus dados com senha
bases sobre NIS. Para se proteger contra isso, o Linux `ypbind` programa oferece a opção de sondar a rede local para localizar o servidor NIS local, ou configurar o nome do servidor NIS em um arquivo de configuração.

NIS + NIS Versus

NIS e NIS + partes pouco mais do que o seu nome e um objetivo comum. NIS + é estruturado de forma inteiramente diferente de NIS. Em vez de um espaço plano com domínios disjuntos NIS, NIS + usa um namespace hierárquico semelhante ao de DNS. Ao invés de mapas, os chamados *tabelas* são utilizados que são compostas de linhas e colunas, em que cada linha representa um objeto no NIS + banco de dados e as colunas de cobrir propriedades dos objetos que conhece e NIS + se preocupa. Cada tabela para um determinado domínio NIS + engloba os domínios do seu pai. Além disso, uma entrada em um tabela pode conter um link para outra tabela. Estas características tornam possível a estrutura de informação de muitas maneiras.

NIS + também suporta RPC seguro e criptografado, o que ajuda muito a resolver os problemas de segurança NIS.

NIS tradicional tem um RPC Número da versão dos dois, enquanto o NIS + é a versão 3. No momento estamos escrevendo, não há
Ainda implementação de um bom trabalho do NIS + para Linux, por isso não é coberto aqui.

O lado do cliente do NIS

Se você estiver familiarizado com a escrita ou portar aplicações de rede, você pode perceber que a maioria dos mapas NIS listados anteriormente correspondem às funções de biblioteca em C da biblioteca. Por exemplo, para obter *passwd* informações, gen-
oralmente usar o *getpwnam* e *getpwuid* funções, que retornam as informações da conta associada ao dado
nome ou identificação numérica do usuário, respectivamente. Em circunstâncias normais, essas funções executar a ação

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

solicitada
pesquisa no arquivo padrão, como */ Etc / passwd*.

Uma implementação NIS conhecimento destas funções, no entanto, modifica seu comportamento e faz uma chamada RPC para o Servidor NIS, que procura o nome ou ID de usuário. Isso acontece de forma transparente para o aplicativo. A função

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

pode tratar os dados NIS como se tivesse sido anexado ao original *passwd* arquivo para os dois conjuntos de informações são disponível para o aplicativo e usados, ou como se ele substituiu completamente de modo que as informações contidas na local *passwd* é ignorada e somente os dados do NIS é usado.

Para implementações tradicionais NIS, houve algumas convenções para que os mapas foram substituídos e que foram anexados à informação original. Alguns, como o *passwd* mapas, modificações necessárias kludgy do *passwd* arquivo que, quando feito de forma incorrecta, abriria brechas de segurança. Para evitar essas armadilhas, a NYS ea GNU *libc* usar um esquema de configuração geral que determina se um determinado conjunto de funções de cliente usa o arquivos originais, NIS ou NIS +, e em que ordem. Este regime será descrito mais tarde neste capítulo.

Executando um servidor NIS

Depois de muito techno teórico-cavaco, é hora de sujar as mãos com o trabalho de configuração real. Neste seção, vamos abordar a configuração de um servidor NIS. Se um servidor NIS está sendo executado em sua rede, você não vai tem que criar o seu próprio, neste caso, você pode seguramente pular esta seção.

Note que se você está indo só para experimentar com o servidor, certifique-se que você não configurá-lo para um domínio NIS nome que já está em uso na sua rede. Isso pode perturbar o serviço de toda a rede e fazer um monte de pessoas muito infeliz e muito irritado.

Existem duas possíveis configurações do servidor NIS: mestre e escravo. A configuração fornece um escravo ao vivo máquina de backup, caso o seu servidor principal falhar. Nós cobriremos a única configuração de um servidor mestre aqui. A documentação do servidor será explicar as diferenças, se você deseja configurar um servidor escravo.

Existem atualmente dois servidores NIS livremente disponível para Linux: uma contidas Tobias Reber *yps* pacote, e o outro em Pedro Eriksson *ypserv* pacote. Não importa qual deles você correr.

Depois de instalar o programa servidor (`ypserv`) Em */ Usr / sbin*, Você deve criar o diretório que vai realizar o mapa de seu servidor de arquivos é distribuir. Ao configurar um domínio NIS para a *cervejaria* domínio, os mapas ia para */ Var / yp / cervejaria*. O servidor determina se é que serve um domínio NIS específico, verificando se o diretório mapa está presente. Se você está desativando alguns serviços de domínio NIS, certifique-se de remover o dihistória também.

Mapas são normalmente armazenados em arquivos DBM para acelerar as pesquisas. Eles são criados a partir do mestre arquivos usando um programa chamado `makedbm` (Para o servidor de Tobias) ou `dbmload` (Para o servidor Pedro).

Transformar um arquivo mestre em uma forma que `dbmload` pode analisar geralmente requer algum `awk` ou `sed` magia, que tende a ser um pouco entediante para escrever e difícil de lembrar. Por isso, Eriksson Pedro *ypserv* pacote contém um Makefile (chamado *ypMakefile*), Que gere a conversão dos arquivos mestres mais comuns para você. Você deve instalá-lo como *Makefile* em seu diretório de mapas e editá-lo para refletir os mapas que você deseja que o servidor NIS para compartilhar. Para a parte superior do arquivo, você vai encontrar o *todos* destino que lista os serviços `ypserv` oferece. Por padrão, o linha é algo como isto:

```
todos: serviços de redes de éteres protocolos hosts rpc passwd grupo netid
```

Se você não quiser produzir, por exemplo, o *ethers.byname* e *ethers.byaddr* mapas, basta remover a *éteres* pré-requisito a esta regra. Para testar sua configuração, você pode começar com apenas um ou dois mapas, como o *serviços.** mapas.

Após a edição do *Makefile*, Enquanto no diretório do mapa, tipo `fazer`. Isto irá gerar automaticamente e instalar os mapas. Você tem que certificar-se de atualizar os mapas sempre que você alterar os arquivos do mestre, caso contrário, o mudanças permanecem invisíveis para a rede.

A seção "Configurando um cliente NIS com GNU libc" irá explicar como configurar o código do cliente NIS. Se a sua configuração não funcionar, você deve tentar descobrir se os pedidos estão a chegar ao seu servidor. Se você especificar o *-depurar* linha de comando-bandeira `ypserv`, Ela imprime mensagens de depuração para o console sobre todos Que NIS-entrada Ries e os resultados retornados. Estes devem dar uma dica de onde reside o problema. servidor Tobias não tem essa opção.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

NIS Server Segurança

NIS costumava ter uma grande falha de segurança: ele deixou o seu arquivo de senha lido por praticamente qualquer pessoa em todo o Inter-
net, o que fez para um grande número de possíveis intrusos. Enquanto um intruso sabia seu nome de domínio NIS eo endereço do seu servidor, ele poderia simplesmente enviar um pedido de *passwd.byname* re mapa e instantaneamente ceive todos do seu sistema de senhas criptografadas. Com um programa rápido de quebra de senha, como `crack` e um bom dicionário, adivinhando, pelo menos, algumas das senhas de seus usuários raramente é um problema.

Isso é o que o *securenets* opção é toda sobre. Ele simplesmente restringe o acesso ao seu servidor NIS para certos hospedeiros, com base
em seus endereços IP ou números de rede. A última versão do `ypserv` implementa esta funcionalidade de duas formas. A primeira se baseia em um arquivo de configuração especial chamado */ Etc / ypserv.securenets* eo segundo utiliza o convenientemente
/ Etc / hosts.allow e */ Etc / hosts.deny* arquivos já encontrados no Capítulo 12, *Rede Características importantes*.[77] Assim, para restringir o acesso a máquinas de dentro da cervejaria, o seu gerente de rede gostaria de acrescentar a seguinte linha *hosts.allow*:

```
ypserv: 172.16.2.
```

Isso permitiria que todos os hosts da rede IP *172.16.2.0* acessar o servidor NIS. Para fechar todos os outros hosts, uma corres-
entrada correspondente em *hosts.deny* teria que ler:

```
ypserv: ALL
```

números de IP não são a única maneira que você pode especificar os hosts ou redes com *hosts.allow* e *hosts.deny*. Consulte o *hosts_access (5)* página de manual do seu sistema para obter detalhes. Entretanto, ser advertido que *não pode* host uso ou nomes de domínio para o *ypserv* entrada. Se você especificar um nome de host, o servidor tenta resolver esse hostname - mas o resolver por sua vez chama `ypserv`, E você cair em um loop infinito.

Para configurar *securenets* segurança com o */ Etc / ypserv.securenets* método, você precisa criar sua configuração arquivo, */ Etc / ypserv.securenets*. Este arquivo de configuração é simples na sua estrutura. Cada linha descreve um host ou rede de hosts que será permitido o acesso ao servidor. Qualquer endereço não descritos por uma entrada neste arquivo será recusada acesso. Uma linha que começa com # será tratado como um comentário. Exemplo 13-1 mostra o que uma simples */ Etc / ypserv.securenets* ficaria assim:

Exemplo 13.1: Exemplo de arquivo ypserv.securenets

```
# Permite conexoes do sistema local - necessários
host 127.0.0.1
# O mesmo que 127.0.0.1 255.255.255.255
#
# Permite conexões de qualquer host na rede Cervejaria Virtual
255.255.255.0   172.16.1.0
#
```

A primeira entrada em cada linha é a máscara de rede usada para a entrada, com *host* sendo tratada como uma palavra-chave especial
que significa "máscara de rede 255.255.255.255." A segunda entrada em cada linha é o endereço IP ao qual pretende aplicar o net-
máscara.

Uma terceira opção é usar o portmapper seguro, em vez do *securenets* opção `ypserv`. O portmap seguro-
por (*portmap-5.0*) Utiliza a *hosts.allow* regime, bem como, mas oferece isso para todos os servidores RPC, e não apenas `ypserv`.[78]
No entanto, você não deve usar os *securenets* opção eo portmapper segura, ao mesmo tempo, por causa da a sobrecarga desta autorização incorre.

~~Configurando um cliente~~ NIS com o GNU libc

Vamos agora descrever e discutir a configuração de um cliente NIS usando o suporte da biblioteca GNU libc.

Seu primeiro passo deve ser para dizer ao cliente NIS GNU libc que servidor usar para NIS serviço. Mencionamos anteriormente que o Linux `ypbind` permite-lhe configurar o servidor NIS de usar. O comportamento padrão é para consulta

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

o servidor na rede local. Se o host que você está configurando é susceptível de passar de um domínio para outro,

77 Para permitir o uso da */ Etc / hosts.allow* método, você pode ter que recompilar o servidor. Por favor, leia as instruções no *README* em concluiu na distribuição.

78 O portmapper seguro está disponível via FTP anônimo *ftp.win.tue.nl* abaixo da */ Pub / security /* diretório.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

como um laptop, você deixaria o */ Etc / yp.conf* arquivo vazio e consulta ia na rede local para a servidor NIS local onde quer que esteja.

A configuração mais segura para a maioria dos Exércitos é para definir o nome do servidor no */ Etc / yp.conf* arquivo de configuração. Um muito simples arquivo para um host na rede da adega pode ser parecido com este:

```
# Yp.conf - Configuração YP para biblioteca GNU libc.
#
vbardolino ypserver
```

A *ypserver* declaração informa ao host para usar o host fornecido como o servidor NIS para o domínio local. Neste exemplo, podemos ter especificado o servidor NIS como *vbardolino*. É claro que o endereço IP correspondente a *vbardolino* deve ser definida na *hosts* arquivo; alternativamente, você pode usar o endereço IP se com a *servidor* argumento.

Na forma mostrada no exemplo, o `ypserver` comando diz `ypbind` para usar o servidor nomeado, independentemente da o que o domínio NIS atual pode ser. Se, no entanto, você está movendo sua máquina entre diferentes domínios NIS com freqüência, você pode querer manter a informação para vários domínios da *yp.conf* arquivo. Você pode ter informações nos servidores para vários domínios NIS em *yp.conf* especificando as informações através da *domínio* declaração. Para exemplo, você pode alterar o arquivo de exemplo anterior para que fique assim por um laptop:

```
# Yp.conf - Configuração YP para biblioteca GNU libc.
#
domínio vbardolino servidor adega
domínio vstout servidor cervejaria
```

Isso permite que você abrir o laptop em qualquer um dos dois domínios, basta definir o domínio NIS desejado na inicialização tempo, através da `domainname` comando. O cliente NIS usa qualquer servidor é relevante para a corrente domínio.

Há uma terceira opção, você pode querer usar. Ele cobre o caso quando você não sabe o nome ou o endereço IP do o servidor para usar em um domínio específico, mas ainda quer a habilidade de usar um servidor fixo em determinados domínios. Imagine queremos insistir em usar um servidor específico, enquanto que operam no domínio da adega, mas quer sonda para o servidor para usar enquanto no domínio Brewery. Gostaríamos de modificar o nosso *yp.conf* arquivo novamente para se parecer com isto:

```
# Yp.conf - Configuração YP para biblioteca GNU libc.
#
domínio vbardolino servidor adega
transmissão de domínio cervejaria
```

A *transmissão* palavra-chave diz `ypbind` para usar qualquer servidor NIS que encontra para o domínio.

Depois de criar este arquivo de configuração básica e ter certeza que ele é lido por todos, você deve executar o primeiro teste para conectar ao seu servidor. Certifique-se de escolher um mapa do seu servidor distribui, como *hosts.byname*, E tentar recuperar lo usando o `ypcat` utilidade:

```
# hosts.byname ypcat
172.16.2.2      vbeaujolais.vbrew.com    vbeaujolais
172.16.2.3      vbardolino.vbrew.com     vbardolino
172.16.1.1      vlager.vbrew.com         vlager
172.16.2.1      vlager.vbrew.com         vlager
172.16.1.2      vstout.vbrew.com         vstout
172.16.1.3      vale.vbrew.com           Vale
172.16.2.4      vchianti.vbrew.com       vchianti
```

A saída que você tem deve lembrar que apenas mostrado. Se você receber uma mensagem de erro ao contrário, que diz: `Não é possível Ligar ao servidor que serve de domínio`, Então o nome de domínio NIS que você definiu não correspondência definida no servidor *yp.conf*, Ou o servidor está inacessível por alguma razão. Neste último caso, certifique-se que um `ping` para o host gera um resultado positivo, e que ele é realmente rodar um servidor NIS. Você pode verificar a esta usando `rpcinfo`, Que deve produzir a seguinte saída:

```
# rpcinfo-u       serverhost       ypserv
versão do programa 100.004 um pronto e esperando
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
versão do programa 100004 2 prontos e à espera
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Escolhendo o direito Maps

Tendo certeza que você pode alcançar o servidor NIS, você tem que decidir quais arquivos de configuração para substituir ou-
mento com os mapas NIS. Geralmente, você vai querer usar os mapas NIS para o host e senha funções de pesquisa.
O primeiro é especialmente útil se você não tem o serviço de nomes BIND. A senha de pesquisa permite que todos os usuários registrar em suas contas a partir de qualquer sistema no domínio do NIS, o que normalmente vai junto com a partilha de uma central */ Home*
directório entre todos os hosts via NFS. O mapa senha é explicado detalhadamente na próxima seção.

Outros mapas, como *services.byname*, Não forneça tais ganhos dramáticos, mas não lhe poupar algum trabalho de edição. A *services.byname* mapa é útil se você instalar todas as aplicações de rede que não use um nome de serviço no nor-
dard *serviços* arquivo.

Geralmente, você quer ter alguma possibilidade de escolher quando uma função de pesquisa utiliza os arquivos locais, quando se

consulta o NIS
servidor, e quando ele usa outros servidores, como DNS. GNU libc lhe permite configurar a ordem em que um fun-
ção de acessos desses serviços. Isso é controlado através do */ Etc / nsswitch.conf* arquivo, que representa *Nome do Serviço Switch*, Mas claro que não se limita ao serviço de nomes. Para qualquer uma das funções de pesquisa de dados suportados pela GNU
libc, o arquivo contém uma linha de nomenclatura dos serviços para uso.

A ordem correta dos serviços depende do tipo de dados de cada serviço está oferecendo. É improvável que o *servi-
vices.byname* mapa vai conter entradas diferentes das do local *serviços* arquivo, que conterá apenas adicio-
entradas internacionais. Assim, parece razoável para consultar os arquivos locais primeiro e NIS verificar se o nome do serviço não é
encontrado. Hostname informações, por outro lado, pode mudar com muita freqüência, então o servidor DNS ou NIS devem ter sempre a conta mais exata, enquanto o local *hosts* arquivo só é mantido como um backup caso o DNS e NIS devem falhar. Para hostnames, portanto, normalmente você deseja verificar o arquivo local passado.

O exemplo a seguir mostra como forçar *gethostbyname* e *gethostbyaddr* olhar no NIS e DNS antes
o *hosts* arquivo e como ter a *getservbyname* função de procurar nos arquivos locais antes de consultar o NIS. Estes funções vão tentar resolver cada um dos serviços listados, por sua vez, se uma pesquisa for bem-sucedido, o resultado é retornado; outras
sábios, eles vão tentar o próximo serviço na lista. O arquivo de configuração para estas prioridades é a seguinte:

```
# Pequena amostra / etc / nsswitch.conf
#
hosts:     nis dns arquivos
serviços:  files nis
```

O seguinte é uma lista completa de serviços e locais que podem ser usados com uma entrada no *nsswitch.conf* arquivo.
Os mapas atuais, os arquivos, servidores e objetos consultados depender do nome de entrada. A seguir podem aparecer à direito de um dois-pontos:

nis

> Use o atual domínio do servidor NIS. A localização do servidor consultado está configurado no *yp.conf* arquivo, como mostrado na seção anterior. Para o *hosts* entrada, o *hosts.byname* e *hosts.byaddr* mapas-que
> Ried.

nisplus ou *nis +*

> Use o NIS + servidor para esse domínio. A localização do servidor é obtido a partir da */ Nis.conf / etc* arquivo.

dns

> Use o nome do servidor DNS. Este tipo de serviço só é útil com o *hosts* entrada. Os servidores de nomes-que
> Ried ainda são determinados pela norma *resolv.conf* arquivo.

arquivos

> Use o arquivo local, como a */ Etc / hosts* arquivo para o *hosts* entrada.

compat

> Ser compatível com os formatos de arquivos mais antigos. Esta opção pode ser usada quando um NYS ou glibc 2.x é
>
> utilizada para
> NIS ou pesquisas. Embora essas versões, normalmente, não pode interpretar as entradas mais antigas NIS em *passwd* e *grupo* arquivos, *compat* opção que lhes permite trabalhar com os formatos.

db

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Procure as informações de DBM arquivos localizados na */ Var / db* diretório. O NIS correspondente mapa nome é usado para esse arquivo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Atualmente, o apoio NIS em GNU libc atende aos seguintes *nsswitch.conf* bases de dados: *aliases*,*ethers*.*group*, *hosts*,*netgroup*,*rede*,*passwd*,*protocolos*,*publickey*,*rpc*,*serviços*E *sombra*. Mais entradas são susceptíveis de ser acrescentou.

Exemplo 13.2 scomos um exemplo mais completo que apresenta uma outra característica da *nsswitch.conf*. A *[Não-ENCONTRADO] = retorno* palavra-chave na *hosts* entrada diz ao cliente NIS a retornar se o item desejado não foi encontrado em
o banco de dados NIS ou DNS. Ou seja, o cliente NIS vão continuar pesquisando os arquivos locais *apenas* se as chamadas para o NIS
e os servidores DNS falhar por algum outro motivo. Os arquivos locais, então, ser usado somente em tempo de boot e como um backup
quando o servidor NIS é baixo.

Exemplo 13.2: Exemplo de arquivo nsswitch.conf

```
# / Etc / nsswitch.conf
#
hosts:      nis dns [NOTFOUND = return] files
redes:      nis [NOTFOUND = return] files
serviços:   files nis
protocolos: files nis
RPC:        files nis
```

GNU libc fornece algumas outras ações que estão descritas na *nsswitch* manpage.

Usando o Maps passwd e grupo

Uma das principais aplicações do NIS é a sincronização de conta de usuário e informações sobre todos os hosts em uma NIS do-principais. Conseqüentemente, você geralmente mantêm apenas um local pequeno */ Etc / passwd* arquivo, a informação que em todo o site da
os mapas NIS é acrescentado. No entanto, simplesmente permitindo NIS pesquisas para este serviço *nsswitch.conf* não é quase o suficiente.

Ao confiar nas informações de senha distribuída pelo NIS, você primeiro tem que se certificar que o usuário numéricos Identificações de todos os usuários que você tem em seu local *passwd* ficheiro de unir a idéia do servidor NIS de IDs de usuário. Coerência no usuário
IDs é importante para outras finalidades também, como montar volumes NFS para outras máquinas na sua rede.

Se algum dos IDs numéricos em */ Etc / passwd* ou */ Etc / group* diferem daquelas nos mapas, você tem que ajustar arquivo posses para todos os arquivos que pertencem ao usuário. Primeiro, você deve mudar todas as UIDs e GIDs em *passwd* e *grupo* para
os novos valores, então, achar que todos os arquivos que pertencem aos usuários apenas mudou e mudar sua propriedade. Assumir
notícias costumava ter um ID de usuário e 9 *okir* tinha um ID de usuário 103, que foram alterados para algum outro valor, você poderia, então, emitir os seguintes comandos como root:

```
#  find /-uid             9-print> / tmp/uid.9
#  find /-uid> 103 impressões / tmp/uid.103
#  cat / tmp/uid.9            | Xargs chown notícias
#  cat / tmp/uid.103 | xargs chown okir
```

É importante que você executar esses comandos com o novo *passwd* arquivos instalados, e que você coletar todos os arquivos nomes antes de alterar a propriedade de nenhum deles. Para atualizar o dono do grupo de arquivos, use um similar método com o GID ao invés do uid e chgrp vez de chown.

Uma vez que você fizer isso, o uids numérica e gids em seu sistema, de acordo com aqueles em todas as outras máquinas na sua Domínio NIS. O próximo passo é adicionar as linhas de configuração para *nsswitch.conf* que permitem NIS pesquisas para o usuário e
informações do grupo:

```
tratamento passwd e grupo - # / etc / nsswitch.conf
nis arquivos: passwd
grupo:  arquivos nis
```

Isso afeta onde o `login` comando e todos os seus amigos procurar informações do usuário. Quando um usuário tenta fazer o login,
`login` irá pesquisar em mapas NIS, primeiro, e se essa pesquisa falhar, ele irá voltar para os arquivos locais. Normalmente, você irá

PDF Creator PDF4Free v2.0 http://www.pdf4free.com

remover
quase todos os usuários de seus arquivos locais, e só deixar as entradas para *root* e contas genéricas como *e-mail* nele. Esta é porque algumas funções vitais do sistema pode ter que uids mapa para usernames ou vice-versa. Por exemplo, administrativa `cron` trabalhos podem executar o *su* comando para tornar-se temporariamente *notícias*Ou o subsistema UUCP pode enviar um status
relatório. Se *notícias* e *uucp* não tiver entradas no local *passwd* arquivo, estes postos de trabalho irá falhar miseravelmente durante um NIS
blecaute.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Por último, se você estiver usando a implementação NIS idade (apoiada pela *compat* modo para a *passwd* e *grupo* arquivos do NYS ou implementações glibc), você deve inserir as entradas pesadas especial para eles. Estes entradas representam onde os registros de NIS derivados serão inseridos no banco de dados de informação. As entradas podem ser adicionado em qualquer lugar, mas geralmente são adicionados ao final. As entradas para adicionar para o */ Etc / passwd* arquivo são:

```
+::::::
```

e para a */ Etc / groups* arquivo:

```
+:::
```

Com ambos a glibc 2.xe NYS você pode substituir os parâmetros no registro de um usuário recebeu do servidor NIS a criação de entradas com um "+" usuários anteposto ao nome de login e excluir especificado através da criação de entradas com um "-" anteposto ao nome de login. Por exemplo, as entradas:

```
+ Bin ::::::/ stuart / JACL
::::::-Jedd
```

seria substituir o shell especificado para o usuário *stuart* fornecidos pelo servidor de NIS, e seria impedir que o usuário *Jedd* de se autenticar nesta máquina. Todos os campos em branco deixado usar as informações fornecidas pelo servidor NIS.

Existem duas grandes ressalvas em ordem aqui. Primeiro, a instalação conforme descrito até aqui só funciona para suites de login que não use senhas shadow. A complexidade de senhas sombra usando o NIS será discutido nos próximos seção. Em segundo lugar, os comandos de login não são os únicos que acessam o *passwd* olhe os - arquivo `ls` comando, que a maioria das pessoas usam quase constantemente. Sempre que compilar uma lista longa, `ls` exibe o símbolo nomes de usuário e grupo donos de um arquivo, ou seja, para cada uid e gid encontra, ele tem que consultar o NIS servidor. Uma consulta NIS leva um pouco mais para fazer do que o equivalente de pesquisa em um arquivo local. Você pode encontrar que partilha a sua *passwd* e *grupo* informações usando o NIS, provoca uma redução perceptível no desempenho das alguns programas que utilizam essas informações com freqüência.

Ainda assim, esta não é toda a história. Imagine o que acontece se um usuário quer mudar sua senha. Normalmente, ela vai invocar `passwd`, Que lê a nova senha e atualiza o local *passwd* arquivo. Isso é impossível com o NIS, desde que o arquivo não está disponível localmente mais, mas os usuários com login no servidor NIS sempre que quiser alterar suas senhas não é uma opção viável. Portanto, NIS fornece um substituto para `passwd` chamada `yppasswd`, Que trata de alterações de senha no NIS. Para alterar a senha na máquina servidora, que contato com o `yppasswdd` daemon em que o anfitrião via RPC, e proporciona-lhe as informações de senha atualizada. Normalmente você instala `yppasswd` sobre o programa normal, fazendo algo parecido com isto:

```
#  cd / bin
#  mv passwd passwd.old
#  ln yppasswd passwd
```

Ao mesmo tempo, você tem que instalar `rpc.yppasswdd` no servidor e iniciá-lo de um script de rede. Este efetivamente ocultar qualquer das contorções do NIS de seus usuários.

Usando o NIS com suporte Shadow

Usando o NIS em conjunto com arquivos de senha sombra é algo problemático. Primeiro, temos uma má notícia: NIS derrotas os objetivos de senhas shadow. A *sombra* esquema de senha foi projetado para evitar que não-usuários de raiz de ter acesso ao formulário de criptografia da senhas de login. Usando o NIS para compartilhar *sombra* dados por necessidade faz com que as senhas criptografadas disponível para qualquer usuário que pode ouvir o servidor NIS respostas sobre o rede. Uma política para impor que os usuários escolham "bom" senhas é indiscutivelmente melhor do que tentar passar-sombra palavras em um ambiente NIS. Vamos dar uma rápida olhada em como fazê-lo, você deve decidir a forjar adiante.

Em libc5 não há solução real para a partilha *sombra* dados usando o NIS. A única maneira de distribuir senha e usuário informações pelo NIS é através do padrão *passwd .** mapas. Se você tem senha oculta instalada, a facil-est maneira de compartilhá-los é gerar um bom *passwd* arquivo da */ Etc / shadow* utilizando ferramentas como `pwuncov`E criar os mapas NIS do arquivo.

Claro, existem alguns hacks necessário o uso de senhas de NIS e sombra ao mesmo tempo, por exemplo, instalação de um */ Etc / shadow* arquivo em cada máquina da rede, enquanto a distribuição de informação do usuário, através do NIS.

No entanto, esse truque é realmente cru e desafia o objetivo de NIS, que é para facilitar a administração do sistema.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O apoio NIS na biblioteca GNU libc (libc6) fornece suporte para bancos de dados de senhas sombras. Não fornecer qualquer solução real para tornar acessíveis as suas senhas, mas não simplificar o gerenciamento de senha

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

ambientes em que você quer usar o NIS com senhas de sombra. Para usá-lo, você deve criar uma *shadow.byname* banco de dados e adicione a seguinte linha ao seu */ Etc / nsswitch.conf*:

```
# Shadow apoio de senha
sombra:                 compat
```

Se você usa senhas shadow junto com o NIS, você deve tentar manter alguma segurança restringindo o acesso a
seu banco de dados NIS. Consulte "Segurança do Servidor NIS", anteriormente neste capítulo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 14 - O Network File System

O Network File System (NFS) é provavelmente o serviço de rede mais proeminente usando RPC. Ele permite que você acessar arquivos em máquinas remotas, exatamente da mesma maneira que você poderia acessar os arquivos locais. Uma mistura de suporte no kernel
e espaço do usuário daemons no lado do cliente, juntamente com um servidor NFS no lado do servidor, torna isso possível. Este acesso ao arquivo é completamente transparente para o cliente e funciona em uma variedade de arquiteturas de servidores e de acolhimento.

NFS oferece uma série de recursos úteis:

- Dados acessados por todos os usuários podem ser mantidos em um host central, com os clientes para montar este

diretório no boot
  tempo. Por exemplo, você pode manter todas as contas de usuário em um host e ter todos os hosts em sua rede montagem */ Home* a partir desse acolhimento. Se o NFS está instalado ao lado do NIS, os usuários podem entrar em qualquer sistema e ainda trabalhar
  em um conjunto de arquivos.

- Dados de consumo de grandes quantidades de espaço em disco podem ser mantidos em um único host. Por exemplo,

todos os arquivos e
  programas relativos ao látex e METAFONT podem ser mantidos em um só lugar.

- Os dados administrativos podem ser mantidos em um único host. Não há necessidade de usar `rcp` para instalar o

mesmo estúpido
  arquivo em 20 máquinas diferentes.

Não é muito difícil de configurar operação NFS básicas sobre o cliente eo servidor, este capítulo informa como.

Linux NFS é em grande parte o trabalho de Rick Sladkey, que escreveu o código do kernel NFS e grandes partes do NFS servidor.[79] Este último é derivado do unfsd espaço do usuário do servidor NFS, originalmente escrita por Mark Shand, e os hnfs Harris servidor NFS, escrito por Donald Becker.

Vamos dar uma olhada em como o NFS trabalha. Em primeiro lugar, um cliente tenta montar um diretório de um host remoto

em um local di-
história do mesmo jeito que faz um dispositivo físico. No entanto, a sintaxe usada para especificar o diretório remoto está diferentes. Por exemplo, para montar */ Home* de acolhimento *vlager* para */ Usuários* em *Vale*, O administrador emite o seguinte comando em *Vale*:[80]

```
# mount-t nfs vlager: / home / usuários
```

`montagem` tentará se conectar ao `rpc.mountd` daemon de montagem em *vlager* via RPC. O servidor irá verificar se *Vale* É permitida a montagem do diretório em questão e, nesse caso, devolvê-lo um identificador de arquivo. Este arquivo identificador será utilizado em
todos os pedidos subsequentes para arquivos abaixo */ Usuários*.

Quando alguém acessa um arquivo sobre NFS, o kernel faz uma chamada RPC `rpc.nfsd` (O daemon NFS) sobre o servidor da máquina. Esta chamada tem o identificador de arquivo, o nome do arquivo a ser acessado, e os IDs de usuário e grupo de
o usuário como parâmetros. Estes são utilizados para determinar os direitos de acesso para o arquivo especificado. A fim de evitar-unau
usuários autorizados de ler ou modificar arquivos de usuários e IDs de grupo deve ser o mesmo em ambos os anfitriões.

Na maioria das implementações do Unix, o NFS funcionalidade de cliente e servidor é implementado como em nível de kernel daemons que são iniciados a partir do espaço do usuário na inicialização do sistema. Estes são os *NFS Daemon* (`rpc.nfsd`) No servidor
de acolhimento, e os *Bloco I / O Daemon* (`biod`) Na máquina cliente. Para melhorar o rendimento, `biod` executa as inter-
~~nous I / O com leitura em frente e w~~rite-behind, também, vários `rpc.nfsd` daemons geralmente são executados simultaneamente.

A implementação do NFS atual do Linux é um pouco diferente do NFS clássico em que o código do servidor é executado inteiramente no espaço do usuário, para execução de várias cópias ao mesmo tempo é mais complicada. O actual `rpc.nfsd` implementação oferece uma funcionalidade experimental que permite suporte multi-processador servidores. Olaf Kirch-devel

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

suporte do servidor desenvolvido baseado no kernel do NFS destaque no kernel 2.2 do Linux versão. Seu desempenho é significativamente
melhor do que a implementação existente userspace. Nós vamos descrevê-lo mais tarde neste capítulo.

79 Rick pode ser alcançado em jrs@world.std.com.

80 Na verdade, você pode omitir o `nfs-t` argumento porque `montagem` vê do cólon que esta especifica um volume NFS.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Preparando NFS

Antes que você possa usar o NFS, seja como servidor ou cliente, você deve se certificar que seu kernel tem suporte NFS compilado dentro
kernels mais novos têm uma interface simples no *proc* sistema de arquivos para isso, o */ Proc / filesystems* arquivo, que pode ser exibição usando `gato`:

```
$ cat / proc / filesystems
        minix
        ext2
        msdos
nodev   proc
nodev   nfs
```

Se *nfs* está faltando nesta lista, você tem que compilar seu próprio kernel com o NFS habilitado, ou, talvez, você vai precisar para carregar o módulo do kernel se o seu suporte NFS foi compilado como um módulo. Configurando a rede do kernel opções é explicado em "Configuração do Kernel" do Capítulo 3, *Configurando o hardware de rede*.

Montando um volume NFS

Os volumes de montagem do NFS se assemelha ao sistema de arquivos regular. Invocar `montagem` utilizando os seguintes sinimposto:[81]

```
# mount-t nfs       nfs_volume opções local_dir
```

nfs_volume é dado como *remote_host*:*remote_dir*. Desde que esta notação é exclusiva para sistemas de arquivos NFS, você pode deixar
o *nfs-t* opção.

Há uma série de opções adicionais que você pode especificar a `montagem` a montagem de um volume NFS. Estes
pode ser concedida após a *-O* ligar a linha de comando ou no campo de opções do */ Etc / fstab* entrada para
o volume. Em ambos os casos, várias opções são separadas por vírgulas e não deve conter nenhum espaço em branco characters. Opções especificadas na linha de comando sempre substituem as constantes do *fstab* arquivo.

Aqui está um exemplo de entrada de */ Etc / fstab*:

```
# Volume              ponto de montagem tipo  opções
news: / var / spool / news              / Var / spool / news      nfs   timeo = 14,
intr
```

Este volume pode ser montado usando o seguinte comando:

```
# montagem news: / var / spool / news
```

Na ausência de um *fstab* entrada, NFS `montagem` invocações de um olhar muito mais feio. Por exemplo, suponha que você montar o seu
diretórios dos usuários a partir de uma máquina chamada *Moonshot*, Que usa um tamanho padrão do bloco de 4 K para leitura / gravação
operações. Você pode aumentar o tamanho da quadra de 8 K para obter um melhor desempenho ao executar o comando:

```
# Moonshot montagem: / home rsize / home-o = 8192, wsize = 8192
```

A lista de todas as opções válidas é descrito em sua totalidade no *nfs (5)* manual de página. A seguir está uma lista parcial dos opções que você provavelmente deseja usar:

n = rsize e *n = wsize*

> Estes especificar o tamanho do datagrama usado pelos clientes NFS sobre os pedidos de leitura e escrita, respectivamente. A
> padrão depende da versão do kernel, mas normalmente é de 1.024 bytes.

n = timeo

> Isso define o tempo (em décimos de segundo), o cliente NFS irá esperar por um pedido para ser concluído. O padrão valor é de 7 (0,7 segundos). O que acontece após um período de tempo depende se você usar o *rígido* ou *moles* opção.

rígido

> Explicitamente marcar este volume tão duro montado. Isto é o padrão, por isso esta opção faz com que o servidor re-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

porta uma mensagem para o console quando o tempo limite ocorre grande e continua tentando indefinidamente.

81 Não se diz, porque estes arquivos não são sistemas de arquivos correta.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

moles

Soft-montagem (em oposição ao hard-mount) o condutor. Esta opção gera um erro de I / O para ser comunicado à processo de tentar uma operação de arquivo quando um tempo limite maior ocorra.

intr

Permitir que os sinais de interromper uma chamada de NFS. Útil para abortar quando o servidor não responde.

Exceto para *rsize* e *wsize*, Todas essas opções se aplicam ao comportamento do cliente se o servidor deve tornar-se-tempo porariamente inacessível. Eles trabalham juntos da seguinte forma: Sempre que o cliente envia uma solicitação para o NFS servidor, ele espera que a operação tiver terminado, após um determinado intervalo (especificado no *timeout* opção). Se não con- a confirmação for recebida dentro deste tempo, o chamado *tempo de espera menor* ocorre, ea operação é repetida com o intervalo de tempo limite dobrado. Depois de atingir um limite máximo de 60 segundos, um *timeout maior* ocorre.

Por padrão, um timeout maior faz com que o cliente deve imprimir uma mensagem para o console e começar tudo de novo, desta vez
com um intervalo inicial de tempo limite de duas vezes maior que a cascata anterior. Potencialmente, isso pode durar para sempre. Volumes
que teimava em repetir a operação até que o servidor estiver disponível novamente são chamados *hard-montado*. A opo- variedade local, chamado *soft-montado*, Gera um erro de E / S para o processo de chamada sempre que ocorre um tempo limite maior.
Devido ao write-behind introduzidas pelo cache de buffer, esta condição de erro não será propagado para o processo se antes ele chama o *escrever* função da próxima vez, portanto, um programa nunca pode ter certeza que uma operação de gravação para um
volume suave montada conseguiu nada.

Quer duro ou mole, montar um volume depende em parte de sabor, mas também sobre o tipo de informação que você quer para acessar a partir de um volume. Por exemplo, se você montar os seus programas de X por NFS, você certamente não quereria sua sessão X para enlouquecer só porque alguém trouxe a rede parar de funcionar por aquecimento acima de sete cópias de Doom, ao mesmo tempo ou puxando o plug Ethernet para um momento. Por rígido de montagem do diretório com esses programas, você se certificar de que o computador espera até que ele é capaz de restabelecer o contato com seu servidor NFS. Por outro lado, os dados não-críticos, tais como NFS-partições montadas notícias ou arquivos FTP também pode ser soft-montado, por isso, se a máquina remota está temporariamente inacessível ou para baixo, não pendurar a sua
sessão. Se a sua conexão de rede com o servidor é esquisito ou passa por um roteador carregado, você pode tanto in- tar o tempo limite inicial com os *timeo* opção ou difíceis de montar os volumes. volumes NFS são difíceis montado por padrão.

Hard monta apresentar um problema, porque, por padrão, as operações de arquivo não são passíveis de interrupção. Assim, se um processo
tentativas, por exemplo, uma gravação para um servidor remoto e que o servidor está inacessível, a aplicação do usuário e trava o usuário não pode fazer nada para abortar a operação. Se você usar o *intr* opção em conjunto com um duro monte, qualquer sinais recebidos pelo processo de interromper o NFS chamada para que os usuários ainda podem abortar acessos a arquivos de suspensão e re-
sume trabalho (embora sem salvar o arquivo).

Normalmente, o `rpc.mountd` daemon, de alguma forma ou de outra se mantém informado dos diretórios que foram montados pelo que hospeda. Esta informação pode ser exibida usando o `showmount` programa, que também está incluído na Pacote de servidor NFS:

```
# Moonshot showmount-
Exportar lista para localhost:
/ Clnt> <anon casa

# showmount-Moonshot d
Diretórios em localhost:
/ Home

# showmount-Moonshot um
Todos os pontos de montagem em localhost:
localhost: / home
```


PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Se você quiser fornecer o serviço de NFS para outras máquinas, você tem que executar o `rpc.nfsd` e `rpc.mountd` daemons em sua máquina. Como os programas baseados em RPC, que não são gerenciados pelo `inetd`, Mas é criada em tempo de inicialização e
registram-se com o portmapper, portanto, você tem que ter certeza para iniciá-los somente após `rpc.portmap` está em execução. Normalmente, você pode usar algo como o exemplo a seguir em uma de sua rede scripts de inicialização:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
if [-x / usr / sbin / rpc.mountd], então
        / Usr / sbin / rpc.mountd echo-n "mountd"
fi
if [-x / usr / sbin / rpc.nfsd], então
        / Usr / sbin / rpc.nfsd echo-n "nfsd"
fi
```

As informações de propriedade dos arquivos de um servidor de NFS oferece aos seus clientes normalmente contém

apenas numérica
IDs de usuário e grupo. Se o cliente eo servidor associa o mesmo usuário e nomes de grupo com essas identificações numéricas, diz-se que o seu uid share / espaço gid. Por exemplo, este é o caso quando você usar o NIS para distribuir o *passwd* informações para todos os hosts em sua rede local.

Em algumas ocasiões, porém, as identificações em diferentes hospedeiros não coincidem. Ao invés de atualizar o UIDs e GIDs

de
o cliente para combinar com as do servidor, você pode usar o `rpc.ugidd` daemon de mapeamento para contornar o disparidade. Usando o *map_daemon* opção explicou um pouco mais tarde, você pode dizer `rpc.nfsd` para mapear o servidor uid / gid do espaço ao espaço uid / gid do cliente com o auxílio do `rpc.ugidd` sobre o cliente. Infelizmente, o `rpc.ugidd` daemon não é fornecida em todas as distribuições Linux modernas, então se você precisar dele e vocês não tem -lo, você precisa compilar o código fonte.

`rpc.ugidd` é um servidor baseado em RPC que é iniciado a partir dos scripts de inicialização de rede, assim como `rpc.nfsd`

e
`rpc.mountd`:

```
if [-x / usr / sbin / rpc.ugidd], então
        / Usr / sbin / rpc.ugidd echo-n "ugidd"
fi
```

As exportações de arquivos

Agora vamos ver como vamos configurar o servidor NFS. Especificamente, nós vamos olhar como nós dizemos que o servidor

NFS
arquivos deve disponibilizar para a montagem, e os diversos parâmetros que controlam a clientes de acesso será que o sistema de arquivos. O servidor determina o tipo de acesso que é permitido para os arquivos do servidor. A */ Etc / exports* arquivo lista os arquivos que o servidor irá disponibilizar para os clientes para montar e usar.

Por padrão, `rpc.mountd` desautoriza todas as montagens do diretório, que é uma atitude pouco sensata. Se você deseja permit um ou mais hospedeiros para NFS-montar um diretório, você deve *exportação* , isto é, especificá-lo na *exportações* arquivo. A sam-
plo arquivo pode ser parecido com este:

```
# Arquivo de exportações para vlager
/ Home            Vale (rw) vstout vlight (rw) (rw)
/ Usr/X11R6       Vale (ro) vstout vlight (ro) (ro)
/ Usr / TeX       Vale (ro) vstout vlight (ro) (ro)
/                 Vale (rw, no_root_squash)
/ Home / ftp      (Ro)
```

Cada linha define um diretório e os anfitriões que têm permissão para montá-lo. Um hostname é geralmente um totalmente

qualificado
nome de domínio, mas pode ainda apresentar as * e *?* coringas, que agem da maneira que fazem com o Bourne shell. Por exemplo, `foo.com laboratório *.` jogos *lab01.foo.com* bem como *laboratory.foo.com*. O anfitrião também pode ser especificados usando uma faixa de endereços IP na forma *endereço/netmask*. Se nenhum nome de host é fornecido, como com o
/ Home / ftp diretório do exemplo anterior, qualquer anfitrião partidas e está autorizado a montar o diretório.

Ao verificar uma série de clientes contra os *exportações* arquivo, `rpx.mountd` olha o nome do endereço do cliente usando o *gethostbyaddr* chamada. Com o DNS, essa chamada retorna hostname canônica do cliente, por isso você deve certificar-se de não usar
aliases em *exportações*. Em um ambiente NIS o nome retornado é o primeiro jogo do banco de dados hosts, e com nem DNS ou NIS, o nome do host retornado é o primeiro encontrado no *hosts* arquivo que corresponde o anúncio do cliente-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

vestido.

O hostname é seguido por uma lista de opcionais separados por vírgula das bandeiras, entre parênteses. Alguns dos valores estes sinalizadores podem tomar são:

seguro

Esta bandeira insiste em que os pedidos sejam feitos de uma porta de origem reservados, ou seja, aquele que for inferior a 1.024. Este
sinalizador é definido por padrão.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

inseguro

Esta bandeira reverte o efeito do *seguro* pavilhão.

ro

Esta flag faz com que a montagem do NFS para ser somente leitura. Esta bandeira é ativado por padrão.

rw

Esta opção monta hierarquia de arquivos de leitura e escrita.

root_squash

Esse recurso de segurança nega a superusuários sobre os hosts especificados quaisquer direitos especiais de acesso pelo mapeamento
pedidos de uid 0 sobre o cliente para o 65534 uid (ou seja, -2) no servidor. Esta identificação deve ser asso-ated com o usuário *ninguém*.

no_root_squash

Não solicitações mapa do uid 0. Esta opção é ativada por padrão, de modo superusuários ter acesso de superusuário para o seu
diretórios exportados sistema.

link_relative

Esta opção converte links simbólicos absolutos (quando o conteúdo link começar com uma barra) em relação links. Esta opção só faz sentido quando todo um conjunto de arquivos é montado, caso contrário, alguns dos ligações podem apontar para nada, ou pior, para arquivos que nunca deveriam ser apontados. Esta opção é ativado por padrão.

link_absolute

Esta opção deixa todas as ligações simbólicas como elas são (o comportamento normal para os servidores Sun fornecidos pelo NFS).

map_identity

Esta opção informa ao servidor para assumir que o cliente usa o mesmo uids e gids como o servidor. Esta op-está ativada por padrão.

map_daemon

Esta opção informa o servidor NFS para assumir que o cliente eo servidor não compartilham a mesma uid / gid espaço. `rpc.nfsd` em seguida, cria uma lista que mapeia as identificações entre cliente e servidor, consultando o do cliente `rpc.ugidd` daemon.

map_static

Esta opção permite que você especifique o nome de um arquivo que contém um mapa estático de UIDs e GIDs. Para ex-amplo, `map_static = / etc / nfs / vlight.map` deve especificar o */ Etc / nfs vlight.map /* arquivo como um
uid / gid mapa. A sintaxe do arquivo de mapa é descrito na *exportações (5)* manual de página.

map_nis

Esta opção faz com que o servidor NIS para fazer o mapeamento de UID e GID.

anonuid e *anongid*

Estas opções permitem que você especifique o uid e gid da conta anônima. Isso é útil se você tiver um volume exportado para o público monta.

Qualquer erro na análise do *exportações* arquivo é relatado para `syslogd`'S *daemon* facilidade ao nível *Advertência* sempre `rpc.nfsd` ou `rpc.mountd` é iniciado.

Note que nomes de host são obtidos a partir do endereço IP do cliente através do mapeamento inverso, de modo a resolver devem ser con-
figurado corretamente. Se você usar o BIND e são muito consciente de segurança, você deve ativar a verificação em sua paródia *host.conf* arquivo. Nós discutimos esses assuntos no capítulo 6, *Nome do serviço e configuração Resolver*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Suporte ao servidor baseado no kernel do NFSv2

O espaço do usuário-servidor NFS tradicionalmente usado no Linux funciona de forma confiável, mas sofre de problemas de

desempenho quando
sobrecarregados. Isto é principalmente devido à sobrecarga da interface chamada de sistema adiciona ao seu funcionamento, e ser-
fazer com que devem concorrer para o tempo com outros, potencialmente menos importantes processos, o espaço do usuário.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O kernel 2.2.0 suporta experimental baseado no kernel do servidor NFS desenvolvidos por Olaf Kirch e mais desenvol-
desenvolvido por HJ Lu, Allan G. Morris, e Myklebust Trond. O kernel baseado em suporte a NFS fornece uma significativa
impulso no desempenho do servidor.

Em distribuições versão atual, você pode encontrar as ferramentas disponíveis no servidor de forma pré-embalada. Se não, você

pode
localizá-los em http://csua.berkeley.edu/ ~ gam3/knfsd /.Você precisará construir um kernel 2.2.0 com o kernel baseado
daemon NFS incluídos, a fim de fazer uso das ferramentas. Você pode verificar se seu kernel tem o daemon NFS-
concluiu, olhando para ver se o */ Proc / sys / sunrpc / nfsd_debug* o arquivo já existe. Se não estiver lá, você pode ter que carregar o
`rpc.nfsd` módulo usando o `modprobe` utilidade.

O kernel baseado daemon NFS usa um padrão */ Etc / exports* arquivo de configuração. O pacote de substituição de consumíveis
versões do `rpc.mountd` e `rpc.nfsd` daemons que você começa da mesma maneira como o seu espaço de usuário
homólogos daemon.

Suporte ao servidor baseado no kernel do NFSv3

A versão do NFS que tem sido mais comumente utilizada é NFS versão 2. A tecnologia tem rolado na frente e
começou a mostrar fragilidades que apenas uma revisão do protocolo poderia superar. A versão 3 da Rede
Sistema de arquivos suporta arquivos maiores e sistemas de arquivos, aumenta a segurança aumentou significativamente, e
oferece uma série de
melhorias de desempenho que a maioria dos utilizadores irão achar útil.

Olaf Kirch e Trond Myklebust estão a desenvolver um servidor NFSv3 experimental. Ele é caracterizado em que o

desenvolvedor
Versão 2.3 do kernel e um patch está disponível contra a fonte do kernel 2.2. Baseia-se na versão 2 baseado no kernel
NFS daemon.

As correções estão disponíveis a partir da base Linux Kernel NFS página inicial do servidor no
http://csua.berkeley.edu/ ~ gam3/knfsd /.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 15 - IPX eo sistema de arquivos NCP

Muito antes de a Microsoft aprendeu sobre redes, e mesmo antes da Internet era conhecido fora acadêmica
círculos, ambientes corporativos, arquivos compartilhados e impressoras com servidores de arquivos e impressão com base na rede Novell
Ware sistema operacional e protocolos associados.[82] Muitos desses usuários corporativos ainda têm redes legadas
com estes protocolos e deseja integrar esse apoio com o seu novo suporte TCP / IP.

O Linux suporta não apenas os protocolos TCP / IP, mas também o conjunto de protocolos utilizados pela Corporação Novell Sistema operacional NetWare. Estes protocolos são primos distantes de TCP / IP, e enquanto eles executam sortes semelhantes de funções, eles diferem em uma série de formas e são, infelizmente, incompatíveis.

O Linux tem duas ofertas de software livre e comercial para fornecer suporte para integração com o Novell pro-
dutos.

Nós vamos apresentar uma breve descrição dos protocolos, neste capítulo, mas nos concentramos em como configurar
e uso de software livre que permite ao Linux para interoperar com produtos da Novell.

Xerox, Novell, e História

Primeiro, vamos olhar para onde os protocolos vieram e como eles se parecem. No final dos anos 1970, a Corporação Xerox
ção desenvolveu e publicou um padrão aberto, chamado de Rede Xerox Specification (XNS). O líquido da Xerox
trabalho de especificação descrita uma série de protocolos projetado para internetworking de propósito geral, com uma forte ênfase na utilização de redes de área local. Havia dois protocolos de rede primária envolvidos: a Internet
Datagram Protocol (IDP), que proporcionou um transporte sem conexão e não confiável de datagramas de um host
para outro, ea Sequenced Packet Protocol (SPP), que era uma forma modificada do IDP, que foi de conexão
base e de confiança. Os datagramas de uma rede XNS foram abordados individualmente. O esquema de endereçamento usado uma combinação de um endereço de 4 bytes da rede IDP (que foi exclusivamente atribuído a cada segmento Ethernet LAN), eo endereço do nó de 6 bytes (o endereço da placa de rede). Roteadores são dispositivos que mudaram datagramas ser-
entre duas ou mais redes separadas IDP. IDP não tem noção de sub-redes, qualquer nova coleção de hosts re-
cadernos outro endereço de rede a ser atribuídos. Os endereços de rede são escolhidos de tal forma que elas são únicas no de redes em questão. Às vezes os administradores desenvolvem convenções fazendo com que cada byte codificar algumas outras informações, tais como localização geográfica, para que os endereços de rede são alocados de forma sistêmica, não é um exigência de protocolo, no entanto.

A Corporação Novell decidiu basear a sua suite de rede própria no conjunto XNS. Novell fez pequenas en-
hancements para IDP e SPP e rebatizou-los IPX (Internet Packet eXchange) e SPX (Sequenced Packet
eXchange). Novell adicionou novos protocolos, como o NetWare Core Protocol (NCP), que forneceu arquivo e
recursos de compartilhamento de impressora que funcionou sobre IPX, eo Service Advertisement Protocol (SAP), o que permitiu hosts
em uma rede Novell para saber quais os hosts que os serviços prestados.

Tabela 15.1 maps a relação entre o XNS, Novell e TCP suites / IP, em termos de função. A relação entre o
os navios são apenas uma aproximação, mas deve ajudá-lo a entender o que acontece quando nos referimos a estes pro-
colos mais tarde.

Tabela 15.1: XNS, Novell e TCP / IP Protocolo de Relacionamento

XNS	Novell	TCP / IP	Características
IDP	IPX	UDP / IP	sem conexão, transporte não confiável
SPP	SPX	TCP	Baseado em conexão, confiável
	PCN	NFS	Arquivo de serviços
	RIP	RIP	Encaminhamento de troca de informações
	SAP		Serviço de troca de informações de disponibilidade

82 Novell e NetWare são marcas registradas da Novell Corporation.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

IPX e Linux

Alan Cox desenvolvido pela primeira vez IPX suporte para o kernel do Linux em 1985.[83] Inicialmente foi útil para pouco mais de roteamento de pacotes IPX. Desde então, outras pessoas, nomeadamente Greg Page, têm dado um apoio adicional.[84] Greg desenvolvidos os utilitários de configuração IPX que usaremos neste capítulo para configurar nossas interfaces. Len Volker-decke apoio desenvolvido para o sistema de NCP para permitir que o Linux para montar volumes sobre o Lucro Líquido conectados à rede,
fileservers Ware.[85] Ele também criou ferramentas que permitem a impressão de e para Linux. Ales Dryak e Martin Stover cada um independentemente desenvolvida PCN daemons servidor de arquivos para Linux que permitem que os clientes conectados à rede NetWare
para montar diretórios do Linux exportado como volumes NCP, assim como o daemon NFS permite que o Linux para servir arquivos
para os clientes usando o protocolo NFS.[86] Caldera Systems, Inc. oferece uma comercial e totalmente licenciada cliente NetWare e um servidor que suporta os mais recentes padrões da Novell, incluindo suporte para o NetWare Directory Service (NDS).[87]

Hoje, portanto, o Linux suporta uma ampla gama de serviços que permitem que os sistemas sejam integrados com os existentes redes Novell baseado.

Suporte Caldera

Embora não detalhe a Caldera suporte NetWare neste capítulo, é importante que falemos sobre ele. Cal-
dera foi fundada por Ray Noorda, ex-CEO da Novell. O Caldera suporte NetWare é um comercial
produto e totalmente suportado pela Caldera. Caldera oferece o suporte NetWare como um componente de sua própria distribuição Linux chamada Caldera OpenLinux. A solução Caldera é uma maneira ideal de introduzir em Linux ambientes que demandam o apoio comercial e capacidade para integrar novos ou já existentes rede Novell obras.

O Caldera suporte NetWare é totalmente licenciada pela Novell, proporcionando um alto grau de certeza que os dois com produtos presas 'serão interoperáveis. As duas excepções a esta certeza são "IP puro" operação para o cliente,
eo servidor NDS, embora nenhum destes estavam disponíveis no momento da escrita. NetWare cliente e NetWare servidor estão ambos disponíveis. Um conjunto de ferramentas de gerenciamento também é fornecido que pode simplificar o gerenciamento de não só
seu sistema operacional Linux baseado em máquinas NetWare, mas suas máquinas Novell NetWare, também, trazendo o poder do Unix
linguagens de script para a tarefa. Mais informações sobre a Caldera podem ser encontradas em seu web site.

Apoio Mais sobre NDS

Junto com a versão 4 do NetWare, da Novell introduziu um recurso chamado de NetWare Directory Service (NDS).
As especificações do NDS não estão disponíveis sem um acordo de confidencialidade, uma restrição que dificulta a desen-
desenvolvimento de suporte gratuito. Somente Versão 2.2.0 ou posterior da *ncpfs* pacote, que discutiremos mais tarde, tem alguma sup-
porta para NDS. Este apoio foi desenvolvido pela engenharia reversa do protocolo NDS. O apoio parece funcionar,
mas ainda é oficialmente considerado experimental. Você pode usar as ferramentas não-NDS NetWare com quatro servidores, desde
eles têm "o modo de emulação de ligação" habilitado.

O software Caldera tem suporte completo para NDS, pois sua aplicação é licenciada da Novell. Este im-
mentação não é livre, no entanto. Então, você não terá acesso ao código fonte e não serão capazes de livremente copiar e distribuir o software.

Configurando o kernel para IPX e NCPFS

Configurando o kernel para o IPX eo sistema de arquivos NCP é simplesmente uma questão de selecionar o kernel apropriado opções em tempo de compilação do kernel. Como com muitas outras partes do kernel, componentes do kernel IPX e NCPFS pode ser
embutido no kernel ou como módulos compilados e carregados usando o `insmod` de comando quando você precisar deles.

As opções a seguir deve ser selecionado se você deseja ter suporte ao Linux e via o protocolo IPX:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Alan pode ser alcançado em alan@lxorguk.ukuu.org.uk.
Greg pode ser alcançado em gpage@sovereign.org.
Volker pode ser alcançado em lendecke@namu01.gwdg.de.
Ales pode ser alcançado em A. Dryak @ sh.cvut.cz. Martin pode ser alcançado em mstover@freeway.de.
Informações sobre Caldera pode ser encontrada em http://www.caldera.com/.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
General setup  --->
    [*] Suporte de Rede


Networking options  --->
    <*> O protocolo IPX

Rede de suporte a dispositivos      --->
    [*] Ethernet (10 ou 100Mbit)
        ... e drivers de dispositivo apropriados Ethernet
```

Se você quiser Linux para apoiar o sistema de arquivos NCP para que ele possa montar volumes NetWare remoto, você deve além-
aliado selecionar as seguintes opções:

```
Filesystems  --->
    [*] / Support proc
    <*> Suporte de arquivo NCP (para montar volumes NetWare)
```

Quando você tiver compilado e instalado o novo kernel, você está pronto para executar IPX.

Configurando Interfaces IPX

Assim como com o TCP / IP, você deve configurar suas interfaces IPX antes que você possa usá-los. O protocolo IPX tem alguns requisitos exclusivos, conseqüentemente, um conjunto especial de ferramentas de configuração foi desenvolvido. Nós iremos usar esses
ferramentas para configurar interfaces IPX e nossas rotas.

Dispositivos de rede de suporte IPX

O protocolo IPX pressupõe que qualquer conjunto de hosts que podem transmitir datagramas para outro sem roteamento pertencem à mesma rede IPX. Todos os hosts pertencentes a um segmento de Ethernet que todos pertencem à mesma rede IPX. Da mesma forma (mas menos intuitiva), ambos os hosts apoiar uma ligação PPP com base em série deve pertencer ao IPX rede que é a ligação em série em si. Em um ambiente Ethernet, há uma série de tipos diferentes de quadros que podem ser usados para transportar datagramas IPX. Os tipos de quadros representam diferentes protocolos Ethernet e descrever
diferentes maneiras de realizar múltiplos protocolos de rede Ethernet mesmo. Os tipos mais comuns de quadro que você vai encontrar são `802.2` e `ethernet_II`. Falaremos mais sobre os tipos de quadro na próxima seção.

Os dispositivos de rede do Linux que atualmente suportam o protocolo IPX são os drivers Ethernet e PPP. A interface Ethernet ou PPP deve estar ativo antes que possa ser configurado para usar IPX. Normalmente, você configurar um Dispositivos Ethernet com IP e IPX, para que o dispositivo já existe, mas se sua rede é somente IPX, você precisa usar o `ifconfig` para mudar o status do dispositivo Ethernet para o seguinte:

```
# ifconfig eth0 up
```

Configuração IPX Tools Interface

Greg Page desenvolveu um conjunto de ferramentas de configuração para interfaces IPX, que é um pacote pré-compilado no

moderno
distribuições e também podem ser obtidos em forma de fonte por FTP anônimo http://metalab.unc.edu/ em o */ Pub / Linux / sistema / arquivos / ncpfs / ipx.tgz* arquivo.

Um *rc* arquivo de script é executado normalmente as ferramentas IPX em tempo de boot. Sua distribuição já pode fazer isso por

você, se você
tenha instalado o software pré-embalados.

O Comando ipx_configure

Cada interface IPX deve saber qual IPX rede a que pertence e que tipo de quadro a ser usado para IPX. Cada host suporte IPX tem pelo menos uma interface que o resto da rede irá utilizar para se referir a ele, conhecido como o *primária* interface. O suporte IPX kernel Linux fornece um meio de configurar automaticamente os parâmetros, o

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`ipx_configure` comando ativa ou desativa o recurso de configuração automática.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Sem argumentos, o `ipx_configure` comando exibe a configuração atual da configuração automática bandeiras:

```
# ipx_configure
Auto Primary Select é OFF
Auto Interface Criar é OFF
```

Tanto o Auto bandeiras Primária e Auto Interface estão desligados por padrão. Para defini-los e permitir configuração automática,
ção, basta fornecer argumentos como estes:

```
# ipx_configure - auto_interface = on - auto_primary = no
```

Quando o `- Auto_primary` argumento é definido como `em`, O kernel automaticamente garantirá que pelo menos um ativo interface funciona como a interface primária para o anfitrião.

Quando o `- Auto_interface` argumento é definido como `em`, O kernel driver IPX vai ouvir todos os quadros recebidos sobre as interfaces de rede ativa e tentativa de determinar o endereço de rede IPX eo tipo de quadro utilizado.

O mecanismo de detecção automática funciona bem em redes geridas correctamente. Às vezes os administradores de rede tomar atalhos e quebrar regras, e isso pode causar problemas para o código de auto-detecção Linux. O mais comum exemplo disso é quando uma rede IPX está configurada para rodar na mesma rede com vários tipos de quadros. Isso é tecnicamente uma configuração inválida, como um 802.2 acolhimento não pode se comunicar diretamente com uma Ethernet II
acolhimento e, portanto, não podem estar na mesma rede IPX. O Linux de software de rede IPX escuta na segmento de datagramas IPX transmitidos sobre ele. Destes, ele tenta identificar quais endereços de rede está em usar e que tipo de quadro é associado com cada um. Se o mesmo endereço de rede está em uso em múltiplos quadros tipos ou em várias interfaces, o código do Linux detecta isso como uma colisão de endereços de rede e é incapaz de determina que é o tipo de quadro correto. Você vai saber que isso está ocorrendo, se você ver mensagens no seu sistema de log que se assemelham:

```
IPX: Rede de colisão número 0x3901ab00
EtherII eth0 e eth0 802.3
```

Se você ver esse problema, desativar o recurso de detecção automática e configurar as interfaces manualmente utilizando o `ipx_interface` comando descrito na próxima seção.

O Comando ipx_interface

A `ipx_interface` comando é usado para adicionar manualmente, modificar e apagar capacidade IPX de uma já existente dispositivo de rede. Você deve usar `ipx_interface` quando o método de configuração automática que acabamos de descrever
não funciona para você, ou se você não quer deixar sua configuração de interface ao acaso. `ipx_interface` permite que você especifique o endereço de rede IPX, o status da interface principal, e IPX tipo de quadro que uma rede device vai usar. Se você estiver criando várias interfaces IPX, você precisa de um `ipx_interface` para cada um.

A sintaxe do comando para adicionar IPX para um dispositivo existente é simples e melhor explicada com um exemplo. Vamos adicionar IPX para um dispositivo de Ethernet existente:

```
# ipx_interface add-p eth0 EtherII 0x32a10103
```

Os parâmetros, por sua vez significa:

-P

Este parâmetro especifica que essa interface deve ser uma interface primária. Este parâmetro é opcional.

eth0

Este é o nome do dispositivo de rede à qual estamos adicionando suporte IPX.

EtherII

Este parâmetro é o tipo de quadro, neste caso Ethernet-II. Esse valor também pode ser codificado como `802.2`, `802.3`Ou `SNAP`.

0x32a10103

Este é o endereço de rede IPX para que essa interface pertence.

O seguinte comando remove IPX de uma interface:

```
# ipx_interface del eth0 EtherII
```

Finalmente, para exibir a configuração atual do IPX um dispositivo de rede, use:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# ipx_interface checar eth0 EtherII
```

A `ipx_interface` comando é explicada com mais detalhes em sua página de manual.

Configurando um roteador IPX

Você vai lembrar de nossa breve discussão dos protocolos utilizados em um ambiente IPX IPX é um roteáveis protocolo e que o Routing Information Protocol (RIP) é usado para propagar informações de roteamento. O IPX versão do RIP é bastante semelhante à versão de IP. Eles operam essencialmente da mesma maneira; roteadores periodicamente transmitir o conteúdo de suas tabelas de roteamento e outros roteadores aprender deles por ouvir e integrar os informação que recebem. Hosts só precisa saber quem é sua rede local e não se esqueça de enviar datagramas para todos outros destinos através de seu roteador local. O roteador é responsável por levar estes datagramas e encaminhamento los para o próximo salto na rota.

Em um ambiente IPX, uma segunda classe de informação deve ser propagada pela rede. O Serviço Anúncio Protocol (SAP) carrega as informações relativas a quais serviços estão disponíveis em que acolhe cerca de da rede. É o protocolo SAP, por exemplo, que permite aos usuários obter listas de servidores de arquivo ou impressão no rede. O protocolo SAP funciona por ter máquinas que prestam serviços de difusão periodicamente a lista de serviços que oferecem. Os roteadores de rede IPX coletar essas informações e propagá-lo em toda a rede com a rede de informações de roteamento. Para ser um roteador IPX compatível, você deve se propagar tanto RIP e SAP da informação.

Assim como IP, IPX no Linux fornece um daemon chamado roteamento `ipxd` para executar as tarefas relacionadas com o

gerenciamento desse
ção de roteamento. Novamente, assim como com o IP, na verdade é o kernel que gerencia o envio de datagramas entre interfaces de rede IPX, mas realiza esta de acordo com um conjunto de regras chamado a tabela de roteamento. A `ipxd` daemon mantém o conjunto de regras até à data, ouvindo em cada uma das interfaces de rede ativas e analisando quando uma mudança de rota é necessária. A `ipxd` daemon também responde a solicitações dos hosts em um diretamente ligado rede que pedir informações de roteamento.

A `ipxd` comando está disponível em pré-embalagens em algumas distribuições, e em forma de fonte por FTP anônimo a partir de http://metalab.unc.edu/ em o */ Pub / Linux / sistema / arquivos / ncpfs / x.xx.tgz-ipxripd* arquivo.

Nenhuma configuração é necessária para a `ipxd` daemon. Quando ele inicia, ele automaticamente gerencia o roteamento entre

as
IPX dispositivos que foram configurados. A chave é assegurar que você tenha os seus dispositivos IPX configurada corretamente usando o `ipx_interface` comando antes de iniciar `ipxd`. Embora a auto-detecção podem funcionar, quando você está exercer uma função de roteamento é melhor não se arriscar, então configurar manualmente as interfaces e salve-se a dor da desagradáveis problemas de roteamento. A cada 30 segundos, `ipxd` redescobre todas as redes conectadas localmente IPX
automaticamente e gerencia-los. Isso fornece um meio de gestão de redes de interfaces que não podem ser ativa de todos os tempos, tais como interfaces PPP.

A `ipxd` normalmente seria iniciado na inicialização de um *rc* script de inicialização assim:

```
# / Usr / sbin / ipxd
```

Não & caráter é necessário porque `ipxd` irá mover-se em segundo plano por padrão. Enquanto o `ipxd` daemon é mais útil em máquinas que funcionam como roteadores IPX, também é útil para os hosts em segmentos onde há vários roteadores presentes. Quando você especificar o `-P` argumento, `ipxd` atuará de forma passiva, ouvindo roteamento em formação do segmento e atualizar as tabelas de roteamento, mas não vai transmitir todas as informações de roteamento. Desta forma, um host pode manter suas tabelas de roteamento atualizadas sem ter de solicitar rotas cada vez que quer contatar um host remoto.

Estático roteamento IPX usando o comando ipx_route

Há ocasiões em que podemos querer codificar uma rota IPX. Assim como com o IP, nós podemos fazer isso com IPX. A `ipx_route` comando escreve uma rota para a tabela de roteamento IPX sem necessidade de ter sido aprendida por o `ipxd` daemon de roteamento. A sintaxe de roteamento é muito simples (desde que não oferece suporte IPX subnetworking) e olha como:

```
# ipx_route adicionar 203a41bc 31a10103 00002a02b102
```

O comando mostrado que adicionar uma rota para a rede IPX remota 203a41bc através do roteador na nossa rede local-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

trabalho 31a10103 com o endereço do nó 00002a02b102.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Você pode encontrar o endereço do nó de um roteador por meio da utilização criteriosa dos `tcpdump` comando com a `-E` ar-
fesa para exibir cabeçalhos de link e olhar para o tráfego do roteador. Se o roteador é uma máquina Linux, você
podem mais simplesmente usar o `ifconfig` comando para exibi-lo.

Você pode excluir uma rota utilizando o `ipx_route` comando:

```
# ipx_route del 203a41bc
```

Você pode listar as rotas que estão ativos no kernel, observando a */ Proc / net / ipx_route* arquivo. Nossa tabela de roteamento

para
muito parecido com este:

```
# ipx_route gato
Rede        Router_Net    Router_Node
203A41BC    31A10103      00002a02b102
31A10103    Diretamente   Conectado
```

O percurso para o 31A10103 rede foi criada automaticamente quando configurada a interface de IPX. Cada um dos
nossas redes locais serão representados por um */ Proc / net / ipx_route* entrada como esta. Naturalmente, se a nossa máquina é
para atuar como um roteador, ele vai precisar de pelo menos uma outra interface.

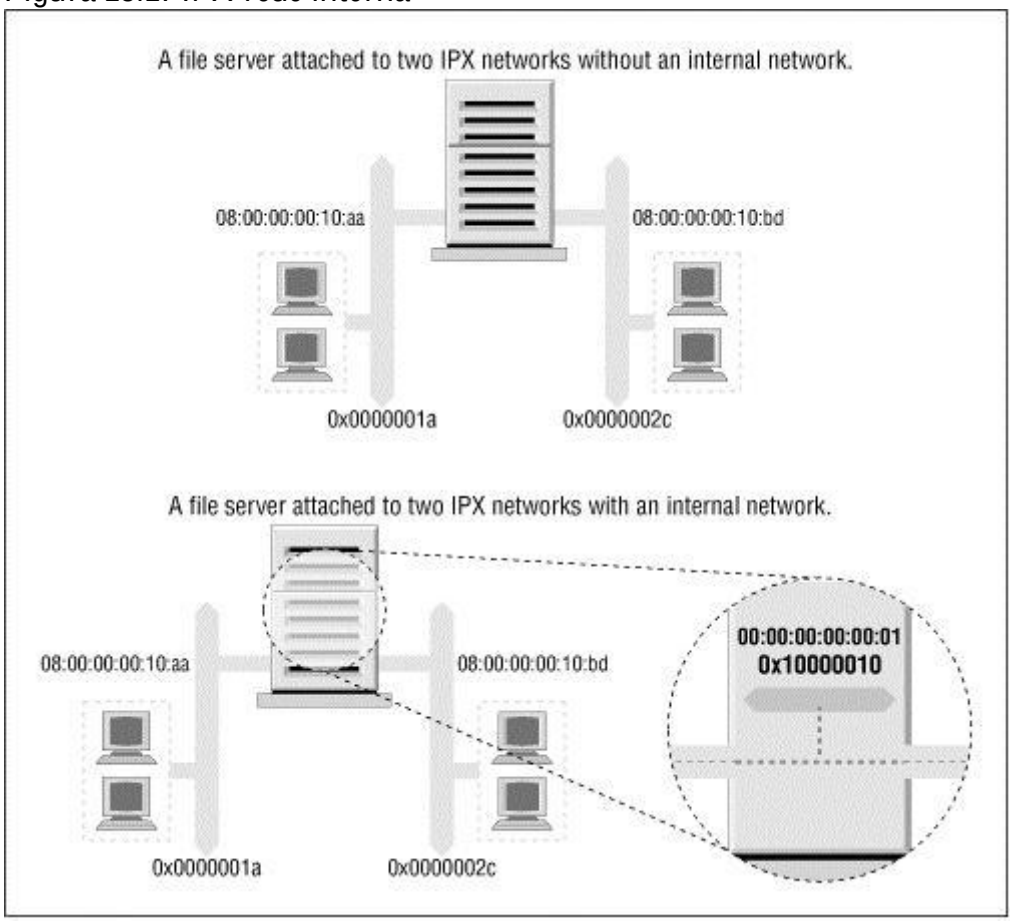
Redes e Roteamento IPX interno

IPX hosts com mais de uma interface IPX possui uma rede exclusiva / combinação de endereço de nó para cada um dos seus
interfaces. Para se conectar a um host, você pode usar qualquer uma dessas redes combinações endereço do nó. Quando a SAP
propaganda de serviços, que fornece o endereço do nó de rede / associado ao serviço que é oferecido. Em hosts
com múltiplas interfaces, isso significa que uma das interfaces deve ser escolhido como o único a se propagar, este é o
função do pavilhão principal interface de que falamos anteriormente. Mas isso apresenta um problema: a rota para esta inter-
cara não pode ser sempre a melhor, e se uma falha de rede que isola a rede do resto do
a rede, o anfitrião se tornará inacessível até que haja outros *possível* rotas para as outras interfaces.
As outras vias não são conhecidos por outros hosts, pois eles nunca são propagadas, eo kernel não tem forma de
sabendo que ela deveria escolher outra interface primária. Para evitar esse problema, foi desenvolvido um dispositivo que
permite que um host IPX para ser conhecido por uma única rede de rotas independentes / endereço do nó para fins de SAP
propagação. Isso resolve nosso problema, porque esta nova rede / endereço do nó é acessível através de todos os host
interfaces, e é o que é anunciado pela SAP.

Para ilustrar o problema e sua solução, Figura 15.1 scomos um servidor conectado a duas redes IPX. O primeiro
rede não tem rede interna, mas a segunda não. O anfitrião no diagrama Figura 15.1 would escolher um dos seus
interfaces como sua interface principal, vamos supor 0000001a: 0800000010aa, E é isso que seria anunciado
como ponto de acesso ao serviço. Isso funciona bem para os hosts da 0000001a rede, mas significa que os usuários sobre a
0000002c via rede através da rede para chegar a esse porto, apesar de o servidor ter uma porta diretamente no que
rede se eles descobriram o servidor das transmissões SAP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Figura 15.1: IPX rede interna



Permitir que esses hosts para ter uma rede virtual com endereços de host virtual que é inteiramente um software de construção resolve este problema. Esta rede virtual é melhor pensado como sendo *dentro* o anfitrião IPX. A informação SAP em seguida, só precisa ser propagada para esta rede virtual / combinação endereço do nó. Esta rede virtual é conhecido como um *rede interna*. Mas como outros hosts saber como alcançar esta rede interna? Remoto hosts rota para a rede interna através de redes conectadas diretamente do hospedeiro. Isso significa que você consulte roteamento entradas que se referem à rede interna de hosts apoiar múltiplas interfaces IPX. Essas rotas deverão escolher a melhor rota disponível no momento, e um deles falhar, o encaminhamento é atualizado automaticamente para a próxima melhor interface e rota. Em Figura 15.1,temos configurada uma rede IPX interno de endereço 0x10000010 e utilizado um endereço do host 00:00:00:00:00:01. É esse endereço que será nossa interface primária e será divulgada via SAP. Nosso encaminhamento irá refletir essa rede, sendo acessível através de *quer* dos nossos portos de rede real, assim Exércitos usar sempre o melhor caminho de rede para se conectar ao nosso servidor.

Para criar esta rede interna, use o `ipx_internal_net` comando incluído nas ferramentas de Greg Página IPX pacote. Novamente, um exemplo simples demonstra a sua utilização:

```
# ipx_internal_net adicionar 10000010 000000000001
```

Este comando criará uma rede IPX interno, com endereço 10000010 e endereço de um nó de 000000000001. O endereço de rede, assim como qualquer outro endereço de rede IPX, deve ser exclusivo na rede. O endereço do nó é completamente arbitrário, como normalmente haverá apenas um nó na rede. Cada host pode ter apenas uma rede interna IPX, e se configurado, a rede interna será sempre o principal líquido-de trabalho.

Para excluir uma rede interna IPX, use:

```
# ipx_internal_net del
```

Uma rede IPX interno é absolutamente inútil para você a menos que o seu acolhimento tanto dispõe de um serviço e tem mais de uma interface IPX ativo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Montagem de um volume NetWare remoto

IPX é comumente usado para montar volumes NetWare no sistema de arquivos Linux. Isto permite com base em arquivo de

compartilhamento de dados
entre outros sistemas operacionais como Linux. Volker Lendecke desenvolveu o cliente NCP para Linux e um conjunto de ferramentas associadas que tornam possível o compartilhamento de dados.

Em um ambiente NFS, que usaria o Linux `montagem` comando para montar o sistema remoto. Infelizmente,
o sistema de arquivos NCP tem necessidades únicas que o tornam impraticável a construí-la no normal `montagem`. Linux tem uma `ncpmount` comando que iremos utilizar. A `ncpmount` comando é uma das ferramentas de Volker *ncpfs* pacote, que está disponível na maioria das distribuições pré-moderna ou em forma de fonte de *ftp.gwdg.de* na */ Pub / linux / misc / ncpfs /* diretório. A versão atual, no momento da escrita é 2.2.0.

Antes que você possa montar volumes NetWare remoto, você deve garantir sua interface de rede IPX está configurada corretamente (conforme descrito anteriormente). Em seguida, você deve saber seus dados de login no servidor NetWare que você deseja
montagem, o que inclui a identificação de usuário e senha. Finalmente, você precisa saber qual o volume que deseja montar e o diretório local que você deseja para montá-lo abaixo.

Um exemplo simples ncpmount

Um exemplo simples de `ncpmount` uso parecido com este:

```
#  ncpmount-S ALES_F1-U rick-P d00-b-gud / mnt / cervejaria
```

Este comando monta todos os volumes do `ALES_F1` fileserver sob a */ Mnt / cervejaria* diretório, usando o Net-login Ware `rick` com a senha `d00-b-gud`.

A `ncpmount` comando é normalmente setuid para *root* e pode, portanto, ser usado por qualquer usuário Linux. Por padrão, que o usuário possui a conexão e só ele ou o *root* usuário será capaz de desmontá-lo.

NetWare incorpora a noção de um *volume*, Que é análogo a um sistema de arquivos no Linux. Um volume NetWare é
a representação lógica de um sistema de arquivos do NetWare, o que poderia ser uma partição de disco único ser espalhado através de muitas partições. Por padrão, o suporte ao Linux NCPFS trata volumes como subdiretórios de um grande sistema de arquivos lógicos representada pelo servidor de arquivos inteiro. A `ncpmount` comando faz com que cada um dos volumes do NetWare fileserver montado para aparecer como um subdiretório sob o ponto de montagem. Isso é conveniente se você quiser acessar todo o servidor, mas por razões de complexidade técnica que você não será capaz de re-exportação desses diretórios usando NFS,
se desejar fazê-lo. Vamos discutir uma alternativa mais complexa, que funciona em torno esse problema em um momento.

O Comando ncpmount em detalhe

A `ncpmount` tem um grande número de opções de linha de comando que permitem que você bastante flexibilidade na forma como você gerenciar o seu PCN monta. Os mais importantes são descritas no Tabela 15.2.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Tabela 15.2: ncpmount Argumentos de Comando

Argumento	Descrição
-S *servidor*	O nome do servidor de arquivos para montar.
-U *user_name*	O ID de usuário NetWare para usar quando o login no servidor de arquivos.
-P *passa-palavra*	A senha para usar o login do NetWare.
-N	Esta opção deve ser usada para logins NetWare que não tem uma senha associada elas.
-C	Este argumento desativa a conversão automática de senhas em maiúsculas.
-C *client_name*	Esta opção permite que você especifique que possui a conexão com o servidor de arquivos. Esta é a utilização ful impressão para NetWare, que discutiremos em mais detalhes posteriormente.
-U *uid*	A identificação do usuário de Linux que deve ser mostrado como o proprietário de arquivos no diretório montado. Se isso não é especificado, o padrão é o ID de usuário do usuário que invoca o `ncpmount` comando.
-G *gid*	O ID do grupo Linux que deve ser mostrado como o proprietário de arquivos no diretório montado. Se isso não for especificado, ele será o padrão para o ID do grupo do usuário que invoca o `ncpmount` comando.
-F *file_mode*	Esta opção permite que você especifique o modo de arquivo (permissões) que os arquivos do montado diretório deve ter. O valor deve ser especificado em octal, por exemplo, `0664`. O permissões que você vai realmente ter são as permissões do arquivo do modo com esta opção mascarados com as permissões que seu ID de logon do NetWare tem para os arquivos do arquivo servidor. Você deve ter direitos sobre o servidor e os direitos especificados por esta opção, a fim de acessar um arquivo. O valor padrão é derivado do atual `umask`.
-D *dir_mode*	Esta opção permite que você especifique as permissões do diretório no diretório montado. É se comporta da mesma maneira como o *-F* opção, exceto que as permissões padrão são derivadas dos atuais `umask`. Executar permissões são concedidas sempre que o acesso de leitura é concedida.
-V *volume*	Esta opção permite que você especifique o nome de um único volume NetWare para montar em o ponto de montagem, ao invés de montar todos os volumes do servidor de destino. Esta opção é necessário se você deseja re-exportar um volume montado NetWare usando NFS.
T *time_out*	Esta opção permite que você especifique o tempo que o cliente NCPFS vai esperar por uma resposta a partir de um servidor. O valor padrão é 60ms eo tempo limite é especificado em centésimos de segundo. Se você tiver problemas de estabilidade com PCN montagens, você deve tentar invincar esse valor.
-R *retry_count*	O código do cliente NCP tenta reenviar datagramas para o servidor uma série de vezes antes de decidir a conexão está morto. Esta opção permite alterar a contagem de repetição de o padrão de 5.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Escondendo a sua senha do NetWare Login

É um pouco de um risco de segurança para estar colocando uma senha na linha de comando, como fizemos com o `ncpmount` comando. Outros ativos, usuários simultâneos pode ver a senha, se acontecer de estar a executar um programa como o `topo` ou `ps`. Para reduzir o risco de ver os outros e roubando senhas de login do NetWare, `ncpmount` é capaz de ler certos detalhes de um arquivo no diretório home do usuário. Nesse arquivo, o usuário mantém o nome de login e senha associados com cada um dos servidores de arquivos que ele ou ela pretende montar. O arquivo é chamado *~ /. NWCLIENT* e deve ter
permissões de `0600` para garantir que outros não podem lê-lo. Se as permissões não estão corretas, o `ncpmount` comando irá recusar usá-lo.

O arquivo tem uma sintaxe muito simples. Todas as linhas que começam com um caractere # são tratadas como comentários e são ignoradas.
O restante das linhas tem a seguinte sintaxe:

fileserver / userid senha

A *fileserver* é o nome do servidor de arquivos de suporte dos volumes que você deseja montar. A *userid* é o login nome da sua conta no servidor. A *senha* campo é opcional. Se não for fornecido, o `ncpmount` comando avisa os usuários para a senha quando eles tentam a montagem. Se o *senha* campo é especificado como o `-` personagem, a senha não é utilizado, o que é equivalente ao `-N` linha de comando argumentos.

Você pode fornecer qualquer número de entradas, mas o campo de servidor de arquivo deve ser único. A entrada fileserver primeiro tem es-
significado social. A `ncpmount` usa o comando `-S` argumento de linha de comando para determinar qual dos entradas em *~ /. NWCLIENT* de usar. Se nenhum servidor é especificado usando o `-S` argumento, a entrada do servidor em primeiro lugar *~ /. NWCLIENT*
Assume-se, e é tratada como seu servidor preferido. Você deve colocar o servidor de arquivos você montar mais freqüentemente em
a primeira posição no arquivo.

Um exemplo mais complexo ncpmount

Vamos olhar mais complexo `ncpmount` exemplo, envolvendo uma série de características que descrevemos. Em primeiro lugar,
vamos construir uma simples *~ /. NWCLIENT* arquivo:

```
# NetWare detalhes de login para a Cervejaria e Adega Virtual
#
# Entrar Cervejaria
ALES_F1/MATT staoic1
#
# Entrar Winery
REDS01/MATT staoic1
#
```

Certifique-se de suas permissões estão corretas:
`$ chmod 600 ~ / NWCLIENT`.

Vamos montar um volume do servidor da Vinícola, sob um subdiretório de um diretório compartilhado, especificando o arquivo e
permissões do diretório para que outros possam compartilhar os dados de lá:

```
$ Ncpmount-S REDS01-V PESQUISA-f-0664 d 0775 / usr / share / adega / dados /
```

Este comando, em combinação com o *~ /. NWCLIENT* arquivo mostrado, seria montar o `PESQUISA` volume da `REDS01` servidor para o */ Usr / share / adega / dados /* diretório usando o ID de login do NetWare `MATT` ea repercussão palavra recuperada a partir do *~ /. NWCLIENT* arquivo. As permissões de arquivos são montados `0664` eo diretório de permissões são `0775`.

Explorando algumas das ferramentas IPX Outros

A *ncpfs* pacote contém uma série de ferramentas úteis que não têm descrito ainda. Muitas dessas ferramentas emular as ferramentas que são fornecidos com o NetWare. Nós vamos olhar para as mais úteis nesta seção.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Lista de servidores

A `slist` comando lista todos os servidores de arquivos acessíveis ao host. A informação é realmente recuperados
mais próximo do roteador IPX. Este comando foi, provavelmente, originalmente destinado a permitir aos usuários ver o que fileservers
estavam disponíveis para montar. Mas tornou-se útil como ferramenta de diagnóstico da rede, permitindo que administradores de rede para ver
onde a informação SAP está sendo propagada:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
$ Slist
NPPWR-31-CD01                                  23A91330  000000000001
V242X-14-F02                                   A3062DB0  000000000001
QITG_284ELI05_F4                               78A20430  000000000001
QRWMA-04-F16                                   B2030D6A  000000000001
VWPDE-02-F08                                   35540430  000000000001
NMCS_33PARK08_F2                               248B0530  000000000001
NCCRD-00-CD01                                  21790430  000000000001
NWGNG-F07                                      53171D02  000000000001
QCON_7TOMLI04_F7                               72760630  000000000001
W639W-F04                                      D1014D0E  000000000001
QCON_481GYM0G_F1                               77690130  000000000001
VITG_SOE MAIL_F4R-                             33200C30  000000000001
```

`slist` não aceita argumentos. A saída exibe o nome do servidor, o endereço de rede IPX, e de acolhimento endereço.

Enviar mensagens para usuários do NetWare

NetWare oferece suporte a um mecanismo para enviar mensagens para usuários registrados. A `nsend` implementa este comando recurso em Linux. Você deve estar conectado ao servidor para enviar mensagens, então você precisa fornecer o fileserver nome e detalhes de login na linha de comando com o usuário destino ea mensagem a ser enviada:

```
# nsend-S vbrew_f1-U gary-P supervisor j0yj0y
        "Juntar-me para uma cerveja antes de fazer as filas de impressão!"
```

Aqui um usuário com o nome de logon `gary` envia um convite tentador para a pessoa que utiliza o `supervisor` conta em o `ALES_F1` fileserver. Nosso servidor de arquivos padrão e as credenciais de login será utilizado se não fornecê-los.

Navegação e manipulando dados de ligação

Cada servidor de arquivos NetWare mantém um banco de dados de informações sobre seus usuários e configuração. Esta base de dados
chamada *encadernação*. Linux suporta um conjunto de ferramentas que permitem que você leia, e se você tem permissões de supervisor
no servidor, para definir e removê-lo. Um resumo destas ferramentas é listado na Tabela 15.3.

Tabela 15.3: Ferramentas de Manipulação de Linux Bindery

Nome do comando	Comando Descrição
`nwfstime`	Exibir ou definir a data de um servidor do NetWare e do tempo
`nwuserlist`	Lista de usuários registrados no em um servidor NetWare
`nwvolinfo`	Mostrar informações sobre volumes NetWare
`nwbocreate`	Criar um objeto de ligação NetWare
`nwbols`	Lista de objetos de ligação NetWare
`nwboprops`	Lista de propriedades de um objeto de ligação NetWare
`nwborm`	Remove um objeto de ligação NetWare
`nwbpcreate`	Criar uma propriedade de ligação NetWare

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Tabela 15.3: Ferramentas de Manipulação de Linux Bindery

Nome do comando	Comando Descrição
`nwbpvalues`	Imprima uma propriedade de ligação do NetWare conteúdo
`nwbpadd`	Defina o valor de uma propriedade de ligação NetWare
`nwbprm`	Remove uma propriedade de ligação NetWare

Impressão em uma fila de impressão NetWare

A *ncpfs* pacote contém um pequeno utilitário chamado `nprint` que envia trabalhos de impressão através de uma conexão a um

PCN
NetWare fila de impressão. Este comando cria a conexão se não existe actualmente e utiliza a *~ /. NWCLIENT*
arquivo que foi descrito anteriormente para esconder o nome de usuário e senha de olhares indiscretos. Os argumentos de linha de comando
usados para gerenciar o processo de login são os mesmos que os utilizados pela `ncpmount`, Por isso não vamos passar por essas novamente aqui. Vamos cobrir as mais importantes opções de linha de comando em nossos exemplos, referem-se ao *nprint (1)* homem
ual página para mais detalhes.

A única opção necessária para `nprint` é o nome do arquivo para impressão. Se o nome indicado é - ou se nenhum arquivo nome é especificado, `nprint` vai aceitar o trabalho de impressão `stdin`. O mais importante `nprint` opções especificar a fila de servidor de arquivos e de impressão ao qual você deseja que o trabalho a ser enviado. Tabela 15.4 listas o mais importante
opções.

Tabela 15.4: nprint comando Opções de linha

Opção	Descrição
-S *server_name*	O nome do servidor de arquivos NetWare apoio a fila de impressão que deseja impressão. Normalmente é conveniente para o servidor para ter uma entrada no *~ /. NWCLIENT*. Este opção é obrigatória.
-Q *queue_name*	A fila de impressão para o qual enviar o trabalho de impressão. Esta opção é obrigatória.
-D *job_description*	Texto que aparecerá na cópia do console de utilidade ao exibir a lista de fila postos de trabalho.
-L *linhas*	O número de linhas por página impressa. Este padrão é 66.
-R *colunas*	O número de colunas por página impressa. Este padrão é 80.
-C *cópias*	O número de cópias do trabalho que será impresso. O padrão é 1.

Um exemplo simples usando `nprint` ficaria assim:

```
$ Nprint-S REDS01 PSLASER-q-c 2 / home matt / ethylene.ps
```

Este comando imprimir duas cópias do arquivo */ Home matt / ethylene.ps* para a impressora chamada PSLASER sobre o `REDS01` fileserver usando um nome de usuário e senha obtida a partir da *~ /. NWCLIENT* arquivo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Usando nprint com a Line Printer Daemon

Você deve estar lembrado nos referimos anteriormente que o *-C* opção para o `ncpmount` é útil para a impressão. Enfim, vamos explicar o porquê e como.

Linux normalmente utiliza software de impressão estilo BSD linha. O daemon de impressora de linha (`lpd`) É um daemon que

controla uma
diretório de spool local para os trabalhos que estão na fila para serem impressos. `lpd` lê o nome da impressora e alguns outros parâmetros,
tros a partir do arquivo formatado especialmente spool e grava os dados para a impressora, opcionalmente, passar os dados pela um filtro para transformar ou manipulá-la de alguma forma.

A `lpd` daemon utiliza um banco de dados simples chamado */ Etc / printcap* para armazenar informações de configuração da

impressora, incluindo
que os filtros são para ser executado. `lpd` geralmente é executado com as permissões de um usuário do sistema especial chamado *lp*.

Você pode configurar `nprint` como um filtro para a `lpd` de usar, que permite aos usuários da sua máquina Linux para a saída diretamente para impressoras remotas hospedado por um servidor de arquivos NetWare. Para fazer isso, o *lp* usuário deve ser capaz de escrever PCN
solicitações para a conexão com o servidor NCP.

Uma maneira fácil de conseguir isso sem que o *lp* do usuário para estabelecer a sua própria conexão e login é especificar *lp* como o proprietário de uma conexão estabelecida por outro usuário. Um exemplo completo de como configurar o Linux sistema de impressão para lidar com trabalhos de impressão dos clientes ao longo do NetWare está relacionada em três etapas:

1. Escrever um script.

   A */ Etc / printcap* arquivo não permite opções a serem fornecidos aos filtros. Portanto, você precisa escrever um pequeno script que invoca o comando que você deseja, juntamente com suas opções. O script envoltório poderia ser tão simples como:

   ```
   #! / Bin / sh
   # P2pslaser - simples script para redirecionar para o stdin
   # PSLASER fila no servidor REDS01
   #
   / Usr / bin / nprint REDS01-S-U-stuart q PSLASER
   #
   ```

   Guarde o script no arquivo */ Usr/local/bin/p2pslaser*.

2. Escreva o */ Etc / printcap* entrada.

   Vamos precisar de configurar o *p2pslaser* script que criamos como a saída do filtro no */ Etc / printcap*. Este ficaria algo como:

   ```
   pslaser | Postscript Impressora Laser hospedada pelo servidor NetWare: \
   : Lp = / dev / null: \
   : Sd = / spool / var / pslaser / lpd: \
   : If = usr/local/bin/p2pslaser /: \
   : Af = / var / log / lp-acct: \
   : Lf = / var / log / lp-erra: \
   : Pl # 66: \
   : Pw # 80: \
   : Pc # 150: \
   : Mx # 0: \
   : Sh:
   ```

3. Adicione o *-C* opção para o `ncpmount`.

   ```
   ncpmount-S REDS01 .... C-lp ....
   ```

   Nossos usuários locais *stuart* deve especificar o *lp* usuário como o proprietário da conexão, quando ele monta o

   controle remoto
   Servidor NetWare.

Agora, qualquer usuário de Linux pode optar por especificar `pslaser` como o nome da impressora ao invocar `lp`. O trabalho de

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

impressão
ser enviados para o servidor NetWare especificado e spool de impressão.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Gestão de filas de impressão

A `pqlist` comando lista todas as filas de impressão disponíveis para você no servidor especificado. Se você não especificar um servidor de arquivos na linha de comando usando o *-S* opção, ou um nome de login e senha, estas serão tomadas a partir da entrada padrão na sua *~/.NWCLIENT* arquivo:

```
# pqlist-S vbrew_f1 U guest-n
Servidor: ALES_F1
Imprimir o nome da fila                          Queue ID
------------------------------------------------ ----------
TESTE                                            AA02009E
Q2                                               EF0200D9
NPI223761_P1                                     DA03007C
Q1                                               F1060004
I-DADOS                                          0D0A003B
NPI223761_P3                                     D80A0031
```

Nosso exemplo mostra uma lista de filas de impressão disponíveis para o `convidado` do usuário na `ALES_F1` fileserver.[88]

Para ver os trabalhos de impressão em uma fila de impressão, utilize o `pqstat` comando. Leva o nome da fila de impressão como um argumento e listas de todos os trabalhos na fila. Você pode, opcionalmente, fornecer um outro argumento que indica quantos dos trabalhos na fila que você gostaria de lista. A saída de exemplo a seguir foi compactado um pouco para ajustar a largura da página de livro:

```
$ Pqstat-S ALES_F1 NPI223761_P1

Servidor: ALES_F1   Fila: NPI223761_P1           Queue ID: 6A0E000C
   Seq  Nome      Descrição                       Status   Forma Job ID
------ --------- ------------------------------- ---------------------
     1  TOTRAN    LyX documento - proposal.lyx    Active      0  02660001
```

Nós podemos ver apenas um trabalho de impressão na fila, propriedade do usuário `TOTRAN`. O resto das opções incluem uma descrição do trabalho, seu status e identificador de seu trabalho.

A `pqrm` comando é usado para remover trabalhos de impressão de uma fila de impressão especificado. Para remover o trabalho na fila nós só obteve o estatuto de, usaríamos:

```
$ Pqrm-S ALES_F1 NPI223761_P1 02660001
```

O comando é bastante simples, mas é desajeitado para usar em uma pressa. Seria um projeto interessante para escrever um roteiro básico para simplificar esta operação.

NetWare Emulation Server

Existem dois emuladores de software livre para servidores de arquivos NetWare no Linux. `lwared` foi desenvolvido pela Ales Dryak e `mars_nwe` foi desenvolvido por Martin Stover. Ambos os pacotes oferecem NetWare elementar emulação de servidor de arquivos em Linux, permitindo que os clientes do NetWare para o Linux montar diretórios exportados como NetWare volumes. Enquanto o `lwared` servidor é mais simples de configurar, o `mars_nwe` servidor é mais completos. A instalação e configuração destes pacotes está além do escopo deste capítulo, mas ambos são descritos no IPX HOWTO.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

88 Parece que os administradores do sistema de amostragem foram algumas das mercadorias da Cervejaria Virtual, antes que eles escolheram alguns desses impressão
nomes de fila. Espero que seus nomes fila de impressão são mais úteis!

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 16 - Gerenciando UUCP Taylor

UUCP foi desenvolvido em finais dos anos setenta por Mike Lesk na AT & T Bell Laboratories para fornecer uma conexão

discada simples
rede através de linhas telefônicas públicas. Apesar da popularidade de conexões PPP e SLIP à Internet,
muitas pessoas que querem ter e-mail e Usenet News em seu computador de casa ainda usar o UUCP porque é muitas vezes mais barato, especialmente em países onde os usuários da Internet têm que pagar por minuto para chamadas locais, ou onde eles não têm um provedor local e deve pagar taxas de longa distância de pedágio para se conectar. Embora existam muitos implementações de UUCP rodando em uma ampla variedade de plataformas de hardware e sistemas operacionais, em geral, eles são altamente compatíveis.

No entanto, como a maioria dos softwares que tem alguma tornar-se "padrão" ao longo dos anos, não há que se UUCP chamaria *o* UUCP. Ele passou por uma evolução constante desde a primeira versão foi implementada em 1976. Cur- atualmente, existem duas espécies principais que diferem principalmente em sua configuração de hardware e suporte. Desses dois,
Existem várias implementações, cada uma variando ligeiramente de seus irmãos.

Uma espécie é conhecida como a Versão 2 UUCP, que remonta a uma implementação 1977 por Mike Lesk, David A. Novitz e Greg Chesson. Embora seja bastante antigo, ainda é freqüentemente usado. Implementações recentes do Ver- Sion 2 proporcionam muito mais conforto do que as espécies mais recentes UUCP fazer.

A segunda espécie foi desenvolvida em 1983 e é comumente referida como BNU (Basic Utilitários de rede) ou HoneyDanBer UUCP. O último nome é derivado do nome dos autores (p. Honeyman, DA Novitz e B.
E. Redman) e muitas vezes é reduzido ainda mais a HDB, que é o termo que usaremos neste capítulo. HDB foi con- percebida para eliminar alguns dos Version 2 UUCP de deficiências. Por exemplo, os protocolos de transferência de novas foram adicionadas,
eo diretório de spool foi dividido de modo que agora existe um diretório para cada site com o qual você tem UUCP tráfego.

A implementação do UUCP atualmente distribuídos com o Linux é Taylor UUCP 1,06, que é a versão deste capítulo está baseado.[89] Taylor UUCP Versão 1.06 foi lançado em agosto de 1995. Além do tradicional con- arquivos de configuração, Taylor UUCP também pode ser compilado para compreender o novo estilo - aka Taylor - configuração
arquivos.

Taylor UUCP normalmente é compilado para HDB compatibilidade, o esquema de configuração Taylor, ou ambos. Porque o regime de Taylor é muito mais flexível e, provavelmente, mais fácil de entender do que a configuração HDB muitas vezes obscuro-
arquivos de configuração, iremos descrever o regime de Taylor abaixo.

Este capítulo não se destina a descrever exaustivamente as opções de linha de comando para os comandos e UUCP o que eles fazem, mas para lhe dar uma introdução sobre como configurar um nó de trabalho UUCP. A primeira seção apresenta uma
breve introdução sobre como UUCP implementa a execução remota e transferência de arquivos. Se você não é inteiramente novo ao UUCP, você pode querer saltar para a seção "Arquivos de configuração do UUCP" mais adiante neste capítulo, o que explica os vários arquivos usados para configurar o UUCP.

Nós, entretanto, supor que você esteja familiarizado com os programas do usuário da suíte de UUCP, `uucp` e `uux`. Para um descrição, consulte as páginas de manual online.

Além dos programas acessíveis ao público `uucp` e `uux`, O pacote UUCP contém uma série de comandos utilizados somente para fins administrativos. Eles são usados para monitorar o tráfego através do UUCP seu nó, remova os arquivos de log antigos,
ou compilar estatísticas. Nenhum destes será descrita aqui, porque eles são periféricos para as principais tarefas do UUCP. Além disso, eles estão bem documentadas e bastante fácil de compreender; consulte as páginas de manual para mais in- formação. No entanto, há uma terceira categoria, que compreendem o real UUCP "cavalos de trabalho." Eles são chamados `uucico` (Onde *Cico* stands para cópia em copy-out), e `uuxqt`, Que executa os trabalhos enviados a partir de sistemas remotos. Nós nos concentramos sobre estes dois programas importantes neste capítulo.

Se você não estiver satisfeito com a nossa cobertura desses temas, você deve ler a documentação que acompanha o pacote UUCP. Este é um conjunto de arquivos Texinfo que descrevem a configuração usando o esquema de configuração Taylor. Você
pode converter os arquivos em um Texinfo `dvi` arquivo usando o `texi2dvi` (Encontrado no pacote Texinfo em seu dis- distribuição) e ver o `dvi` arquivo usando o `xdvi` comando.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

UUCP Guylhem Aznar-HOWTO é uma boa fonte para informações sobre o UUCP em um ambiente Linux. Ele está disponível em qualquer espelho Projeto de Documentação do Linux e é enviada regularmente para comp.os.linux.answers.

[89] Escrito e de propriedade de Ian Taylor, 1995.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Há também um fórum de discussão para a discussão de UUCP comp.mail.uucp chamado. Se você tiver perguntas específicas para
Taylor UUCP, você pode ser melhor para pedir-lhes que, ao invés de sobre o comp.os.linux .* grupos.

Transferências UUCP e execução remota

O conceito de trabalho é vital para compreender o UUCP. Qualquer transferência que um usuário inicia com `uucp` ou `uux` é chamada `Emprego`. É constituído por um comando a ser executado em um sistema remoto, uma coleção de arquivos a serem trans-
ridos entre os sites, ou ambos.

Como exemplo, o comando a seguir faz UUCP copiar o arquivo *netguide.ps* para um host remoto chamado *pablo* e executar o `lpr` comando em *pablo* para imprimir o arquivo:

```
$ uux-r pablo! lpr! netguide.ps
```

UUCP não costuma chamar o sistema remoto imediatamente para executar um trabalho (ou então você pode se contentar com `kermit`). Em vez disso, ele armazena temporariamente a descrição do trabalho de distância. Isso é chamado *spool*. A árvore de diretórios
em que os trabalhos são armazenados por isso é chamado o *diretório de spool* e geralmente está localizado na */ Var / spool / uucp*. Em
nosso exemplo, a descrição do trabalho deverá conter informações sobre o comando remoto para ser executado (`lpr`), do usuário que solicitou a execução, e um par de outros itens. Além da descrição do trabalho, tem UUCP para armazenar o arquivo de entrada *netguide.ps*.

A localização exacta e nomeação dos arquivos de spool pode variar, dependendo de algumas opções em tempo de compilação.

HDB-
UUCPs compatível geralmente armazenar arquivos de spool em um */ Var / spool / uucp* subdiretório com o nome do site remoto. Quando compilado para a configuração de Taylor, UUCP cria subdiretórios abaixo do diretório de spool site específico para o diferentes tipos de arquivos de spool.

Em intervalos regulares, disca UUCP o sistema remoto. Quando uma conexão com a máquina remota é estabelecida, UUCP transfere os arquivos de descrição do trabalho, mais quaisquer arquivos de entrada. Os trabalhos recebidos não serão executadas ime-
diatamente, mas somente depois que a conexão termina. A execução é tratada por `uuxqt`, Que também cuida de for-
defender todos os trabalhos que são designados para um outro local.

Para distinguir entre mais e menos importantes trabalhos associados, UUCP um *grau* com cada trabalho. Este é um único dígitos variando de 0 a 9, de A a Z e A a Z, em precedência decrescente. Mail é costumeiramente
enrolado com grau B ou C, enquanto a notícia é enrolado com grau N. Jobs com notas mais altas são transferidos anteriormente. Grades podem ser atribuídos usando o *-G* sinalizador quando invocando `uucp` ou `uux`.

Você também pode proibir a transferência de postos de trabalho abaixo de um determinado grau, em determinados momentos.

Para isso vamos definir o *máxima*
spool grau que será proibido durante uma conversa. O máximo de spool padrão da classe A a Z, ou seja, todos os notas serão transferidos a cada vez. Nota da ambigüidade semântica aqui: um arquivo é transferido somente se tiver um grau *igual a* ou *acima* o limite máximo do carretel grau.

O funcionamento interno do uucico

Para entender o porquê `uucico` precisa saber uma informação, uma rápida descrição de como ele realmente con-
NECTS para um sistema remoto é útil.

Quando você executa `uucico -s`*sistema* a partir da linha de comando, `uucico` primeiro tem que conectar fisicamente. A ações tomadas dependerão do tipo de conexão para abrir. Assim, ao usar uma linha telefônica, tem que encontrar um mo-
DEM e marcar. Sobre o TCP, ele tem que chamar *gethostbyname* para converter o nome para um endereço de rede, descobrir qual porta abrir, e vincular o endereço para a tomada correspondente.

Uma conexão bem-sucedida é seguido por autorização. Este procedimento consiste geralmente do sistema remoto pedindo um nome de login e possivelmente uma senha. Esta troca é comumente chamado de *sessão de bate-papo*. A au-
zação procedimento é realizado tanto pelo costume `Getty Images / login` conjunto, ou em sockets TCP `uucico` em si.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Se
autorização tiver êxito, o terminal remoto acionado até `uucico`. A cópia local do `uucico` que iniciou a liga-
ção é referido como *mestre*E cópia do controle remoto como *escravo*.

Em seguida vem a *fase de handshake*: O mestre envia ao seu nome acrescido de várias bandeiras. O escravo verifica esse host
nome permissão para log in, enviar e receber arquivos, etc As bandeiras descrever (entre outras coisas) o máximo
grau de arquivos de spool para transferência. Se ativado, a contagem de uma conversa ou *número de seqüência chamada*
verificação tem lugar aqui.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Com esse recurso, os dois sites manter uma contagem de conexões bem-sucedidas, que são comparados. Se eles não partida, o aperto de mão não. Isso é útil para se proteger contra impostores.

Finalmente, os dois `uucico`s tentar chegar a um comum *protocolo de transferência de*. Este protocolo regula a forma como os

dados são
transferidos, verificados quanto à consistência, e retransmitidas, em caso de erro. Há uma necessidade para os diferentes protocolos
por causa dos tipos diferentes de conexões aceitas. Por exemplo, linhas telefônicas exige um protocolo "seguro", que é pessimista sobre os erros, enquanto a transmissão TCP é inerentemente confiável e pode usar um mais eficiente protocolo que renuncia a verificação de erros mais extra.

Após o aperto de mão é concluída, a fase de transmissão propriamente dita. Ambas as extremidades ativar o protocolo

selecionado
motorista. Neste ponto, os motoristas possivelmente realizar uma seqüência de inicialização do protocolo específico.

O mestre então envia todos os arquivos em fila para o sistema remoto, cujo grau de spool é alta o suficiente. Quando se tem acabados, informa o escravo que é feito e que o escravo pode agora desligar. O escravo agora pode concordar para desligar ou assumir a conversa. Esta é uma mudança de papéis: agora o sistema remoto torna-se mestre e o local torna-se escravo. O novo mestre agora envia seus arquivos. Quando terminar, tanto `uucico`Termina troca-s ção de mensagens e fechar a conexão.

Se precisar de informações adicionais sobre o UUCP, consulte o código-fonte. Há também um artigo muito antigo flutuando em torno da Net, escrito por David A. Novitz, o que dá uma descrição detalhada do protocolo UUCP.[90] O Taylor UUCP FAQ também discute alguns detalhes de implementação do UUCP. É colocada comp.mail.uucp regularmente.

uucico Opções de linha de comando

Nesta seção, descrevemos as mais importantes opções de linha de comando para `uucico`:

- - Sistema de sistema,-s

Chama o chamado *sistema* menos que proibido por restrições de tempo de permanência.

-S do sistema

Chama o chamado *sistema* incondicionalmente.

- Mestre,-R1

Inicia `uucico` em modo master. Este é o padrão quando *-S* ou *-S* é dado. Todos os documentos por si só, a *-R1* opção causas `uucico` para tentar chamar todos os sistemas do *sys* arquivo descrito na próxima seção deste capítulo, menos que proibido por chamada ou repetição restrições de tempo.

- Escravo,-r0

Inicia `uucico` no modo escravo. Este é o padrão quando não há *-S* ou *-S* é dado. No modo escravo, quer stan- dard entrada / saída são assumidos para ser conectado a uma porta serial ou a porta TCP especificada pelo *-P* op- ção é usada.

- Ifwork,-C

Esta opção de suplementos *-S* ou *-S* e diz `uucico` chamar o sistema chamado apenas se existirem postos de trabalho spool para ele.

tipo-debug, X-TYPE -,X-TYPE

Ativa a depuração do tipo especificado. Vários tipos podem ser dadas como uma lista separada por vírgulas. A tipos a seguir são válidos: *anormais*,*chat*,*aperto de mão*,*uucp proto-*,*proto*,*porto*,*config*,*spooldir*,*executar*, *entrada*E *saída*. Usando *todos* gira em torno de todas as opções. Para compatibilidade com execução UUCP outras ções, um número pode ser especificado ao contrário, que gira em torno de depuração para o primeiro *n* itens acima lista.

Mensagens de debug serão registrados no *Depurar* arquivo abaixo */ Var / spool / uucp*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

90 Também é incluído no 4.4BSD *Manual do Sistema Gerenciador de*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Arquivos de configuração do UUCP

Ao contrário dos programas mais simples transferência de arquivos, o UUCP foi projetado para ser capaz de lidar com todas as

transferências automaticamente.
Uma vez configurado corretamente, a interferência do administrador não deve ser necessária no dia-a-dia. A informações necessárias para a transferência automatizada é mantido em um par de arquivos de configuração que residem no */ Usr / lib / uucp* diretório. A maioria destes arquivos são usados apenas quando a ligação.

Uma introdução suave para Taylor UUCP

Para dizer que a configuração do UUCP é difícil seria um eufemismo. É realmente um sujeito cabeludo, e os às vezes o formato concisa dos arquivos de configuração não torna as coisas mais fáceis (embora o formato Taylor é al- leitura mais fácil em comparação com os formatos antigos de HDB ou Versão 2).

Para lhe dar uma idéia de como todos os arquivos de configuração interagir, vamos apresentar-lhe as mais importantes e ter um olhar para exemplos de entradas a partir desses arquivos. Não iremos explicar tudo em detalhes agora, uma avaliação mais precisa
conta está em seções separadas que se seguem. Se você deseja configurar sua máquina para o UUCP, você teve melhor começar com alguns arquivos de exemplo e adaptá-las gradualmente. Você pode escolher qualquer um desses abaixo ou os incluídos na sua distribuição Linux favorita.

Todos os arquivos descritos nesta seção são mantidos em */ Etc / uucp* ou em um subdiretório do mesmo. Algumas distribuições

Linux con-
tain binários UUCP que têm suporte para HDB e configuração Taylor habilitado, e usar subdivisões diferentes reitorias para cada arquivo de configuração do conjunto. Geralmente, há uma *README* arquivo em */ Usr / lib / uucp*.

Para o UUCP para funcionar corretamente, esses arquivos devem ser possuídos pelo *uucp* usuário. Alguns deles contêm as

senhas e
números de telefone, e, portanto, deve ter permissões de 600. Observe que, embora a maioria dos comandos UUCP deve ser setuid para *uucp*, Você deve certificar-se da `uuchk` programa é *não*. Caso contrário, os usuários serão capazes de exibir senhas do sistema, embora os arquivos de modo 600.

O arquivo de configuração central é UUCP */ Etc / uucp / config*, Que é usada para definir parâmetros gerais. O mais im- portante deles (e por agora, a única) é o nome do seu anfitrião UUCP. Na Cervejaria Virtual, eles usam *vstout* como seu gateway UUCP:

```
# / Etc / uucp / config - UUCP arquivo de configuração principal
nodename         vstout
```

A *sys* é o arquivo de configuração importante seguinte. Ele contém todas as informações específicas do sistema de sites para qual está vinculado. Isso inclui o nome do site e informações sobre a ligação em si, tais como o telefone número quando se usa um link de modem. Uma entrada típica para um site chamado modem conectado *pablo* ficaria assim:

```
# / Usr / lib / uucp / sys - nome de vizinhos UUCP
# Sistema: pablo
sistema         pablo
tempo           Qualquer
telefone        555-22112
porto           serial1
velocidade      38400
chat            ogin: ssword vstout: lorca
```

tempo especifica as vezes em que o sistema remoto pode ser chamado. *chat* descreve os scripts de login de bate-papo - o seqüência de seqüências que devem ser trocadas para permitir `uucico` para entrar no *pablo*. Nós entraremos em contato para conversar scripts
mais tarde. A *porto* palavra-chave simplesmente nomes uma entrada no *porto* arquivo. (Consulte a Figura 16.1.) Você pode atribuir qualquer
nome que quiser, contanto que se refere a uma entrada válida no *porto*.

A *porto* arquivo contém informações específicas para o próprio link. Para as ligações de modem, ele descreve o arquivo de

dispositivo especial para
ser utilizado, a gama de velocidades suportadas, eo tipo de marcação equipamento conectado à porta. Os seguintes entrada descreve / Dev / ttyS1 (Aka COM 2), a que o administrador tenha ligado um modem Hayes Smartmodem 2400 ou Well

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

de correr a velocidades de até 38.400 bps. O nome da porta é escolhida para coincidir com o nome da porta dada no *sys* arquivo:

```
# / Etc / uucp / porta - as portas UUCP
# / Dev/ttyS1 (COM2)
porto           serial1
tipo            modem
dispositivo     / Dev/ttyS1
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
velocidade      38400
discador        nakwell
```

As informações referentes ao dialers é mantido em outro arquivo chamado - você adivinhou - *dial*. Para cada um discador tipo, ele basicamente contém a seqüência de comandos que são emitidos para dial-up de um site remoto, dado o telefone número. Novamente, isso é especificado como um script de chat. Por exemplo, a entrada para NakWell pode ter este aspecto:

```
# / Etc / uucp / dial - informação por discadores
# Modems NakWell
discador        nakwell
chat            "" AT & F OK ATDT \ T CONNECT
```

A linha de partida com *chat* especifica o modem de bate-papo, que é a seqüência de comandos enviados e recebidos do modem para inicializá-lo e torná-lo discar o número desejado. A \ *T* seqüência será substituído pelo número de telefone `uucico`.

Para lhe dar uma idéia aproximada como `uucico` lida com esses arquivos de configuração, suponha que você emitir o seguinte comando:

```
$ s uucico-pablo
```

A primeira coisa `uucico` faz é olhar para cima *pablo* na *sys* arquivo. A partir da *sys* entrada do arquivo para *pablo*, Ela vê que ele
deve usar o *serial1* porta para estabelecer a conexão. A *porto* arquivo informa `uucico` que esta é uma porta do modem, e que tem um modem NakWell anexado.

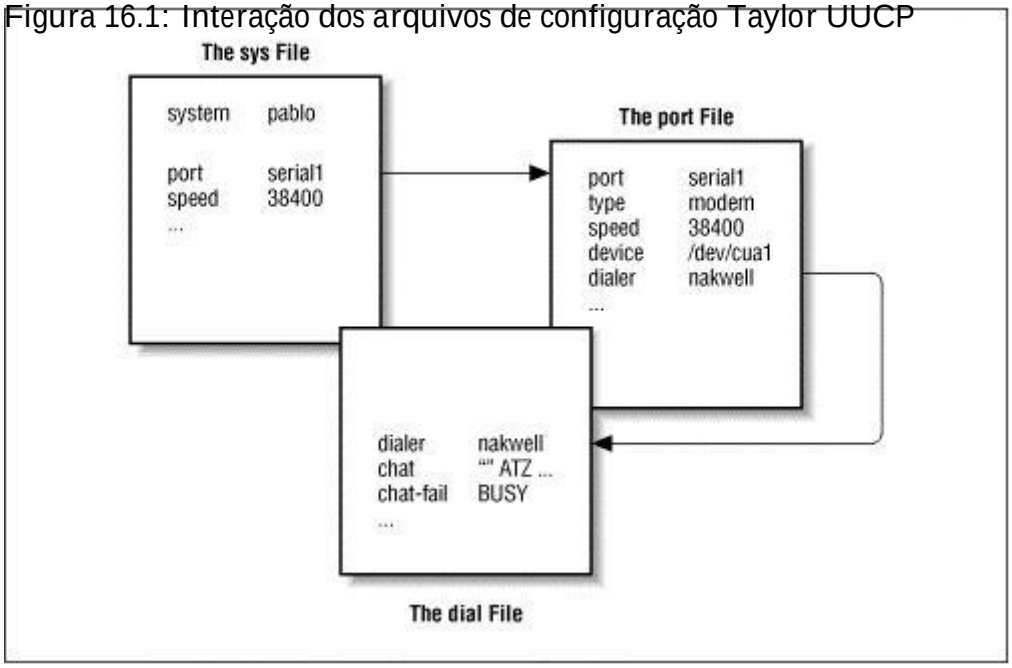
`uucico` agora procura *dial* para a entrada descrevendo o modem NakWell e, tendo encontrado uma, abre a série porto */ Dev/cua1* e executa o discador chat. Ou seja, ele envia `AT & F`, Espera o `OK` resposta, etc Quando deparo--registo das cordas \ *T*, Que substitui o número do telefone (555-22112) extraídos da *sys* arquivo.

Após o retorno do modem `CONNECT`, A conexão foi estabelecida, eo modem de bate-papo está completa. `uucico` agora retorna ao *sys* arquivo e executa o login chat. No nosso exemplo, seria aguardar o `login:` alerta, em seguida, enviar o seu username (vstout), Aguardar o `senha:` prompt, e enviar a sua senha (`lorca`).

Depois de completar a autorização, o fim remoto é assumido ao fogo até o seu próprio `uucico`. Os dois então entrar na fase de handshake descrito na seção anterior.

Figura 16.1 illudemonstra as dependências entre os arquivos de configuração.

Figura 16.1: Interação dos arquivos de configuração Taylor UUCP



PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O UUCP Precisa Saber

Antes de começar a escrever os arquivos de configuração do UUCP, você tem de reunir algumas informações que UUCP requer.

Primeiro, você tem que descobrir qual o dispositivo de série do seu modem está conectado. Geralmente, as portas (DOS) COM1: COM4: mapa para os arquivos do dispositivo especial */ Dev/ttyS0* através */ Dev/ttyS3*. Algumas distribuições, como o Slackware, criar um link chamado */ Dev / modem* para o adequado *ttyS* * dispositivo, arquivo e configurar `kermit`,`seyon`E quaisquer outros programas de comunicação para usar este arquivo genérico. Neste caso, você deve usar */ Dev / modem* em seu UUCP configuração também.

A razão para usar um link simbólico é que todos os programas de discagem utilizar os chamados *arquivos de bloqueio* para sinalizar quando uma série porta está em uso. Os nomes desses arquivos de bloqueio são uma concatenação de string *LCK ..* eo dispositivo de arquivo, para instância *LCK .. ttyS1*. Se os programas usam nomes diferentes para o mesmo dispositivo, eles vão deixar de reconhecer uns dos outros arquivos de bloqueio. Como conseqüência, eles vão atrapalhar uns aos outros a sessão quando iniciado ao mesmo tempo. Isto é bastante possível quando você programar sua UUCP chamadas usando um *crontab* entrada. Para mais detalhes sobre a configuração da porta serial, consulte o Capítulo 4, *Configurando o Hardware Serial*.

Em seguida, você deve descobrir a que velocidade o modem e Linux irão se comunicar. Você tem que definir essa velocidade para a taxa de transferência máxima efetiva você espera obter. A taxa efetiva de transferência pode ser muito maior do que o taxa de transferência física primas modem é capaz. Por exemplo, muitos modems enviar e receber dados a 56 kbps. Usando protocolos de compressão, tais como V.42bis, a taxa de transferência real pode subir mais de 100 kbps.

Claro que, se o UUCP é fazer alguma coisa, você precisa do número do telefone de um sistema de chamada. Além disso, você precisa de um ID de logon válido e, possivelmente, uma senha para a máquina remota.[91]

Você também tem que saber *exatamente* como entrar no sistema. Você tem que pressionar a tecla Enter antes do login prompt aparece? Será que ele exiba `login:` ou `usuário:`? Isso é necessário para compor o *chat script*. Se você não sabe, ou se o script habitual bate-papo falhar, tente chamar o sistema com um programa de terminal como `kermit` ou `minicom` e registrar exatamente o que você tem que fazer.

Site Naming

Tal como acontece com redes TCP / IP, o host tem que ter um nome para a rede UUCP. Contanto que você simplesmente quer usar o UUCP para transferências de arquivos ou de sites que você discar diretamente, ou em uma rede local, este nome não não têm de cumprir todas as normas.[92]

No entanto, se você usar o UUCP para um link de correio ou de notícias, você deve pensar em ter o nome registrado com o UUCP Projeto de Mapeamento.[93] O UUCP Mapping Project é descrito no Capítulo 17, *Correio Eletrônico*. Mesmo se você participar de um domínio, você pode considerar ter um nome UUCP oficial do seu site.

Freqüentemente, as pessoas escolhem o seu nome UUCP para coincidir com o primeiro componente do seu nome de domínio totalmente qualificado. Suponha que o seu endereço de domínio do site é *swim.twobirds.com*E, depois, o seu hostname UUCP seria *nadar*. Pense UUCP sites como conhecer uns aos outros em uma base do primeiro-nome. Claro, você também pode usar um nome totalmente UUCP alheios ao seu nome de domínio totalmente qualificado.

No entanto, certifique-se de não usar o nome do site não qualificados em endereços menos que você tenha registrado como seu UUCP nome oficial. Na melhor das hipóteses, e-mail para um host UUCP unregistered irá desaparecer em alguns pouco grande e preto balde. Se você usar um nome já na posse de algum outro site, este e-mail será encaminhado para o site e fazer a sua pós-mestre de muitas dores de cabeça.

Por padrão, o pacote UUCP usa o nome definido pelo `hostname` como o nome do site UUCP. Este nome é normalmente

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

definido por um comando no tempo de boot *rc* scripts, e é normalmente armazenado no */ Etc / hostname*. Se seu nome é UUCP diferente do que você definir o hostname, você tem que usar o `hostname` opção no *config* arquivo para contar `uucico` sobre o seu nome UUCP. Isto é descrito a seguir.

91 Se você está indo só para experimentar o UUCP, obter o número de arquivo de um site perto de você. Anote o login e senha - que são públicos para fazer downloads anónimos possível. Na maioria dos casos, eles são algo como *uucp / uucp* ou *nuucp / uucp*.

92 A única limitação é que não deve ser superior a sete personagens, de modo a não confundir o UUCP implementações que são executados em uma ope- AVALIAR sistema que impõe um limite estreito em nomes de arquivos. Nomes que são mais de sete personagens são geralmente truncados por UUCP. Alguns versões até mesmo limitar o nome a seis caracteres.

93 O UUCP Projeto de Mapeamento registra todas UUCP hostnames em todo o mundo e garante que eles são únicos.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Arquivos de configuração Taylor

Voltamos agora para os arquivos de configuração. Taylor UUCP obtém suas informações dos seguintes arquivos:

config

Este é o principal arquivo de configuração. Você pode definir o nome do seu site UUCP aqui.

sys

Este arquivo descreve todos os sites conhecidos. Para cada site, especifica seu nome, quais os tempos de chamá-lo, o que núme-
ber para marcar (se houver), que tipo de dispositivo de usar, e como efetuar o logon.

porto

Este arquivo contém entradas que descrevem cada porta disponível, juntamente com a velocidade da linha de suporte e discador para ser usado.

dial

Este arquivo descreve dialers usada para estabelecer uma conexão telefônica.

dialcode

Este arquivo contém expansões para códigos de discagem simbólico.

chamada

Este arquivo contém o nome de login e senha a ser utilizada quando se chama um sistema. Raramente é utilizado.

passwd

Este arquivo contém os nomes de login e senhas que os sistemas podem utilizar para exploração madeireira polegadas
Ele é usado apenas
quando `uucico` faz a sua verificação de senha própria.

Taylor arquivos de configuração são geralmente constituídas por linhas contendo valor pares de palavras-chave. Um sinal de
hash introduz
um comentário que se estende até o final da linha. Para usar um cardinal para significar-se, fugir com uma barra invertida como isso: \ #.

Há um bom número de opções que você pode sintonizar com estes arquivos de configuração. Não podemos entrar em todos os
parâmetros,
tros, mas vamos cobrir os mais importantes aqui. Então você deve ser capaz de configurar um modem baseado em UUCP link. Cortes adicionais descrever as modificações necessárias se você quiser usar o UUCP sobre TCP / IP ou através de uma linha direta de série. A referência completa é dada no Texinfo documentos que acompanham a Taylor fontes de UUCP.

Quando você pensa que você tenha configurado o seu sistema UUCP completamente, você pode verificar a configuração usando o `uuchk` ferramenta (localizado no */ Usr / lib / uucp*). `uuchk` lê arquivos de configuração e imprime um relatório detalhado da configuração de valores utilizados para cada sistema.

Geral Configuração de opções usando o arquivo de configuração

Você não vai usar esse arquivo, geralmente para descrever muito ao lado de seu hostname UUCP. Por padrão, usará o UUCP nome definido com o `hostname` comando, mas é geralmente uma boa idéia para definir o nome UUCP explicitamente. Aqui está um exemplo *config* arquivo:

```
# / Usr / uucp / lib / config - UUCP arquivo de configuração principal
hostname        vstout
```

Uma série de parâmetros variados podem ser ajustadas aqui também, como o nome do diretório de spool ou acesso direitos para o UUCP anônimo. Este último será descrito mais tarde neste capítulo na seção "Anónimo UUCP. "

How to Tell UUCP sobre outros sistemas usando o arquivo sys

A *sys* arquivo que descreve os sistemas de sua máquina conhece. Uma entrada é introduzido pela *sistema* -chave

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

palavra, as linhas subseqüentes até a próxima *sistema* detalhe da directiva, os parâmetros específicos para esse site. Comumente, uma
entrada do sistema define parâmetros como o número de telefone e login de bate-papo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Parâmetros antes da primeira *sistema* linha de definir valores padrão usado para todos os sistemas.

Geralmente, você define o protocolo
parâmetros e como na secção de padrões.

Os campos mais importantes são discutidos em detalhe nas secções seguintes.

nome System

A *sistema* nomes de comando no sistema remoto. Você deve especificar o nome correto do sistema remoto, não um alias que você inventou, porque `uucico` irá verificar se contra o que o sistema remoto diz que é chamado quando você log em.[94]

Cada nome de sistema pode aparecer apenas uma vez. Se você quiser usar vários conjuntos de configurações para o mesmo

sistema
(Tais como os diferentes números de telefone `uucico` deve tentar, por sua vez), você pode especificar *suplentes*, Que vamos de-
escriba, após as opções de configuração básica.

O número de telefone

Se o sistema remoto está a ser atingido por uma linha telefônica, o *telefone* campo especifica o número do modem deve discar. Ele pode conter vários símbolos interpretados por `uucico`É procedimento de marcação. Um sinal de igual (=) significa
aguarde o tom de discagem secundário, e um traço (-) gera uma pausa de um segundo. Algumas instalações telefónicas engasgar quando você não pausa entre a marcação de um código especial de acesso eo número de telefone.[95]

Muitas vezes, é conveniente usar nomes ao invés de números para descrever os códigos de área de marcação. A *dialcode* arquivo

permite
você associar um nome com um código que pode posteriormente ser usado ao especificar números de telefone para re-
hosts mote. Suponha que você tenha o seguinte *dialcode* arquivo:

```
# / Usr / lib / uucp / dialcode - tradução dialcode
Bogoham         024881
Coxton          035119
```

Com estas traduções, você pode usar um número de telefone, como *Bogoham7732* na *sys* arquivo, que provavelmente tornar as coisas um pouco mais legível e um lote inteiro mais fácil de atualizar, se o código de discagem para Bogoham sempre mudar.

porta e velocidade

A *porto* e *velocidade* opções são usadas para selecionar o dispositivo usado para chamar o sistema remoto eo máximo velocidade com que o dispositivo deve ser definido.[96] A *sistema* entrada pode usar tanto a opção por si só ou ambas as opções em con-
ção. Ao olhar-se um dispositivo adequado no *porto* arquivos, apenas os portos que têm um nome de porta de correspondência e / ou velocidade
gama são selecionados.

Geralmente, usando o *velocidade* opção só deve ser suficiente. Se você tiver apenas um dispositivo serial definido no *porto*, `uucico` sempre escolhe o caminho certo mesmo, então você só tem que dar a velocidade desejada. Se você tiver vários modems conectados a seus sistemas, muitas vezes você ainda não quiser nomear um porto particular, porque se `uucico` encontra
que há várias partidas, ele tenta cada dispositivo, por sua vez, até encontrar a que não utilizado.

A sessão de bate-papo

Nós já encontramos o login script de conversação, o que diz `uucico` como entrar no sistema remoto. É constituída de uma lista de tokens especificando seqüências esperadas e enviados pelo local `uucico` processo. `uucico` aguarda até que a máquina remota envia um prompt de login, em seguida, retorna o nome de login, aguarda que o sistema remoto para enviar a passagem
alerta da palavra, e envia a senha. Espere cordas e enviar aparecem em alternância no script. `uucico`
anexa automaticamente um caractere retorno de carro (\ *R*) Para enviar qualquer string. Assim, um simples script de bate-papo olharia
como:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
ogin: ssword vstout: Catch22
```

Você provavelmente vai perceber que o espere que os campos não contêm todo o solicita. Isso garante que o login bem-CEEDS, mesmo se o sistema remoto transmite `Login:` em vez de `login:`. Se a string que você está esperando ou enviá-ção contém espaços ou outros caracteres espaço em branco, você deve usar aspas ao redor do texto.

94 Versão mais antiga do 2 UUCPs não transmitam o seu nome ao ser chamado, no entanto, as implementações mais recentes costumam fazer, e assim faz Taylor UUCP.

95 Por exemplo, as instalações da maioria das empresas privadas é necessário discar 0 ou 9 para obter uma linha para o exterior.

96 A taxa de bits do *tty* deve ser pelo menos tão alta quanto a velocidade de transferência máxima.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`uucico` também permite algum tipo de execução condicional. Digamos que a máquina remota `getty` precisa ser reset antes de enviar um alerta. Para isso, você pode anexar um subchat a uma seqüência de esperar, partiu de um traço. O sub-bate-papo é executado somente se o principal esperar falhar, ou seja, ocorre um tempo limite. Uma maneira de utilizar esse recurso é para enviar uma
Quebrar se o site remoto não exibir um prompt de login. O exemplo a seguir dá um propósito geral de bate-papo script que deve funcionar também no caso de você ter que pressionar Enter antes do login aparece. O argumento vazio em primeiro lugar, `""`, Diz o UUCP não esperar por nada, mas para continuar com a próxima seqüência enviar:

```
"" \ N \ r \ d \ r \ n \ c ogin:-BREAK ogin: ssword vstout: Catch22
```

Um par de cordas especiais e caracteres de escape podem ocorrer no chat script. A seguir está uma lista parcial dos caracteres legais em esperar strings:

`""`

A cadeia vazia. Diz `uucico` de não esperar por nada, mas para prosseguir com a im próxima seqüência envio mediata.

\ T

Caractere de tabulação.

\ R

Transporte de caracteres de retorno.

\ S

Espaço personagem. Você precisa disto para inserir espaços em uma seqüência de bate-papo.

\ N

Nova linha de caracteres.

*\ *

Backslash caráter.

Em enviar cadeias, os caracteres de escape a seguir e as cordas são legais, além do acima:

EOT

Fim da transmissão de caracteres (`^ D`).

BREAK

Ruptura do caráter.

\ C

Suprimir o envio de retorno de carro no final da cadeia.

\ D

Atrasar o envio de um segundo.

\ E

Ativar o eco de controlo. Isto requer `uucico` para aguardar o eco de tudo o que ele escreve para ser lido trás do aparelho antes que ele possa continuar com o bate-papo. É útil principalmente quando usado em modem Bate-papo (o que vamos encontrar mais tarde). verificação Echo está desativado por padrão.

\ E

Desativar o eco de controlo.

\ K

O mesmo que *BREAK*.

\ P

Pausa para uma fração de segundo.

Suplentes

Às vezes você quer ter várias entradas para um único sistema, por exemplo, se o sistema pode ser alcançado em diferentes linhas de modem. Com Taylor UUCP, você pode fazer isso através da definição de um chamado *suplente*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Uma entrada alternativo retém todas as configurações a partir da entrada principal do sistema e especifica apenas os valores que devem ser
substituído na entrada padrão do sistema ou adicionados a ela. Uma alternativa é compensar a entrada do sistema por um con-
line
neamente o palavra-chave *suplente*.

Para usar dois números de telefone para *pablo*, Você poderia modificar a sua *sys* entrada da seguinte forma:

```
sistema      pablo
telefone     123-456
.. entradas como acima ...
suplente
telefone     123-455
```

Ao chamar *pablo*,`uucico` marca primeiro 123-456, e se isso falhar, ele tentará o suplente. A entrada alternativo
retém todas as configurações a partir da entrada principal do sistema e substitui o número de telefone.

Restringindo vezes chamada

Taylor UUCP fornece um número de maneiras que você pode restringir os horários em que as chamadas podem ser colocados

para um sistema remoto
tem. Você pode fazer isso por causa das limitações dos lugares host remoto em seus serviços durante o horário comercial,
ou simplesmente para evitar vezes com taxas de chamadas. Observe que sempre é possível substituir as restrições de tempo de permanência por
dando- `uucico` o *-S* ou *-F* opção.

Por padrão, Taylor UUCP não permite conexões a qualquer momento, assim que você *ter* usar algum tipo de especificação de

tempo
na *sys* arquivo. Se você não se importa com chamadas restrições de tempo, você pode especificar o `tempo` opção com um valor de *Qualquer*
em seu *sys* arquivo.

A maneira mais simples para restringir o tempo de chamada é incluir um *tempo* entrada, seguido por uma cadeia formada por um

dia e uma hora
subcampo. Dia pode ser qualquer combinação de *Mo, Tu, Nós, Th, Fr, Sa,* e *Su*. Você também pode especificar *Qualquer*,*Nunca*Ou *Wk* para os dias úteis. O tempo consiste em dois valores de 24 horas, separados por um traço. Eles especificar o intervalo durante o qual podem ser colocados. A combinação destes símbolos é escrito sem espaços em branco entre eles.
Qualquer número de especificações de data e hora podem ser agrupados por vírgulas, como mostra esta linha:

```
tempo            MoWe0300-0730, Fr1805-2200
```

Este exemplo permite que as chamadas às segundas e quartas-feiras, 03h00-07h30, e às sextas-feiras entre
06:05 pm e 10:00 pm Quando um tempo de domínio da meia-noite se estende, por exemplo *Mo1830-0600*, Que significa realmente segunda-feira, ser-
entre meia-noite e 6h00 e entre as 18:30 ea meia-noite.

O especial de seqüências de tempo *Qualquer* e *Nunca* dizer o que eles dizem: As chamadas podem ser colocados em qualquer ou

nenhum tempo, respectivamente.

Taylor UUCP também tem uma série de símbolos especiais que você pode usar em seqüências de tempo, como *Menor atividade*

e *Noite*.
Estes símbolos especiais são sinónimos de *Any2300-0800, SaSu0800-1700* e *Any1800-0700, Sasu*, Respectivamente.

A *tempo* comando leva um segundo argumento opcional que descreve uma repetição de tempo em minutos. Quando uma

tentativa de
estabelecer uma conexão falhar, `uucico` não permitirá uma nova tentativa de discagem para o host remoto dentro de um certo intervalo. Por exemplo, quando você especificar uma repetição de tempo de 5 minutos, `uucico` se recusam a chamar o sistema remoto
dentro de 5 minutos após a última falha. Por padrão, `uucico` utiliza um esquema de backoff exponencial, onde a repetição aumenta a cada intervalo de incumprimento reiterado.

A `timegrade` comando permite anexar um carretel grau máximo a um cronograma. Por exemplo, suponha

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

você tem o seguinte `timegrade` comandos em um *sistema* entrada:

```
timegrade           Wk1900 N-0700, Sasu
timegrade           C Qualquer
```

Isso permite que os trabalhos com um grau de carretel de C ou superior (geralmente mail está na fila com grau B ou C) para ser transferido
sempre que uma chamada é estabelecida, enquanto as notícias (geralmente na fila com N ª série) são transferidos apenas durante a noite e nos fins de semana.

Assim como `tempo`, O `timegrade` comando tem um intervalo de repetição em minutos, como um terceiro argumento opcional.

No entanto, uma ressalva sobre as notas de spool está em ordem aqui. Primeiro, o `timegrade` opção se aplica apenas ao que *sua*
sistemas envia, o sistema remoto pode ainda transferir o que quiser. Você pode usar o `chamada-timegrade` op-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

ção explicitamente pedido para envio de trabalhos apenas a partir de algum grau de spool dado, mas não há garantia de que vai obedecer
este pedido.[97]

Da mesma forma, o *timegrade* campo não é verificada quando um sistema remoto de chamadas, de forma alguma os trabalhos

em fila para a convocação
sistema será enviado. No entanto, o sistema remoto pode solicitar explicitamente a sua `uucico` limitar-se a um certo grau de spool.

Identificação Dispositivos Disponíveis Através da porta Arquivo

A *porto* arquivo informa `uucico` sobre as portas disponíveis. Estes são normalmente portas de modem, mas outros tipos, como de linhas de série e sockets TCP, também são suportadas.

Como o *sys* arquivo, *porto* consiste em separar as entradas começando com a palavra-chave *porto* seguido pelo nome do porto.

Este
nome pode ser usado na *sys* arquivo *porto* declaração. O nome não precisa ser exclusivo, se existem várias portas com o mesmo nome, `uucico` vou tentar um de cada vez até encontrar um que não está sendo usado atualmente.

A `porto` comando deve ser seguido imediatamente pela *tipo* declaração, que indica o tipo de porta é
descrito. Os tipos válidos são *modem,directo* para conexões diretas, e *tcp* para sockets TCP. Se o `porto` comando estiver ausente, o padrão tipo de porta de modem.

Nesta seção, iremos cobrir apenas as portas do modem, as portas TCP e linhas directas são discutidos em uma seção posterior.

Para modem e portas direto, você tem que especificar o dispositivo de chamada, utilizando a *dispositivo* directiva. Normalmente, este é o nome de um arquivo de dispositivo especial na */ Dev* diretório, como */ Dev/ttyS1*.

No caso de um dispositivo de modem, a entrada do porto também determina que tipo de modem está conectado à porta. Dif-
diferentes tipos de modems têm de ser configurado de forma diferente. Mesmo modems que se dizem compatíveis com Hayes nem sempre são realmente compatíveis com o outro. Portanto, você tem a dizer `uucico` como inicializar o mo-
dem e torná-lo discar o número desejado. Taylor UUCP mantém as descrições de todos os marcadores em um arquivo chamado *dial*.
Para usar qualquer uma dessas, você tem que especificar o nome do discador usando a `discador` comando.

Às vezes, você vai querer usar um modem de diferentes maneiras, dependendo de qual sistema você chamar. Por exemplo, alguns modems mais antigos não entendem quando um modem de alta velocidade tenta se conectar a 56 kbps, elas simplesmente soltar a linha, em vez de negociar um contato em 9.600 bps, por exemplo. Quando você sabe site *queda* usa tal
modem muda, você tem que configurar o modem ao chamá-los de forma diferente. Para isso, você precisa de um adicional porta de entrada na *porto* arquivo que especifica um comunicador diferente. Agora você pode dar o novo porto um nome diferente, tais
como *serial1 lenta*E usar o *porto* directiva no *queda* entrada do sistema em *sys*.

A melhor distinguir as portas é pelas velocidades que eles suportam. Por exemplo, as duas entradas da porta para o acima situação pode ser parecido com este:

```
# Modem NakWell; contato em alta velocidade
porto           serial1         # Nome da porta
tipo            modem           # Modem
dispositivo     / Dev/ttyS1     # Isto é COM2
velocidade      115200          # Suportados velocidade
discador        nakwell         # Discador normal
# NakWell modem, ligue em baixa velocidade
porto           serial1         # Nome da porta
tipo            modem           # Modem
dispositivo     / Dev/ttyS1     # Isto é COM2
velocidade      9600            # Suportados velocidade
discador        nakwell lenta   # Não tente rápido contato
```

A entrada do sistema para site *queda* passaria a dar *serial1* como o nome da porta, mas o pedido de usá-lo em apenas 9.600 bps. `uucico` em seguida, usa automaticamente a segunda porta de entrada. Todos os restantes sítios que têm uma velocidade de 115.200 bps em
a entrada do sistema será chamado utilizando a primeira porta de entrada. Por padrão, a primeira entrada com uma velocidade compatível será

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

utilizado.

97 Se o sistema remoto é executado Taylor UUCP, que vai obedecer.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Como discar um número usando o botão Arquivo

A *dial* arquivo descreve a forma como são utilizados diversos discadores. Tradicionalmente, as negociações

UUCP de discadores e não mo-
dems, porque nos tempos antigos, era prática usual ter um (caro) do dispositivo de discagem automática servir a um
banco inteiro de modems. Hoje, a maioria dos modems de discagem têm suporte integrado, para que esta distinção fica um pouco
turva.

No entanto, discadores diferentes ou modems podem exigir uma configuração diferente. Você pode descrever cada um deles na *dial* arquivo. As inscrições no *dial* começar com o `discador` comando que dá nome ao discador do.

A entrada mais importante, além `discador` é o modem chat, especificado pela `chat` comando. Semelhante ao sessão de bate-papo, ele consiste de uma seqüência de strings `uucico` envia para o discador e as respostas que espera em troca. É comumente utilizada para redefinir o modem a um estado conhecido e discar o número. O exemplo a seguir *discador* entrada mostra um modem típico papo de um modem compatível com Hayes:

```
# Modem NakWell; contato em alta velocidade
discador        nakwell         # Nome do discador
chat            "" AT & F OK \ r ATH1E0Q0 ATDT OK \ r \ T CONNECT
bate-papo não   BUSY
bate-papo não    ERRO
bate-papo não    NO \ sCARRIER
dtr-toggle      verdade
```

O modem começa com bate-papo `""`, O vazio espera string. `uucico` portanto, envia o primeiro comando `AT & F` imediatamente. `AT & F` Hayes é o comando para reiniciar o modem para a configuração padrão de fábrica. `uucico` em seguida,
espera até que o modem tenha enviado `OK` e envia o comando seguinte, que desliga o eco local e afins. Depois os retornos modem `OK` novamente, `uucico` envia o comando de discagem `ATDT`. A seqüência de escape `\ T` nessa seqüência é substituído pelo número de telefone tomadas a partir da entrada do sistema *sys* arquivo. `uucico` em seguida, aguarda o modem
retornar a string `CONNECT`, O que indica que uma conexão com o modem remoto foi estabelecida su-
com sucesso.

Às vezes o modem não conseguir se conectar ao sistema remoto, por exemplo, se o outro sistema está conversando com alguns, uma pessoa ea linha está ocupada. Neste caso, o modem retorna uma mensagem de erro indicando o motivo. Modem bate-papos não são capazes de detectar essas mensagens; `uucico` continua a aguardar o string esperado até que o tempo para fora. O arquivo de log UUCP, portanto, apenas mostra uma branda "expirou no chat script" em vez da razão específica.

No entanto, Taylor UUCP lhe permite dizer `uucico` sobre essas mensagens de erro usando o `bate-papo não` com-
mando como mostrado acima. Quando `uucico` detecta um bate-papo não seqüência ao executar o modem de bate-papo, ele aborta a
chamada e registra a mensagem de erro no arquivo de log UUCP.

O último comando no exemplo acima, diz o UUCP para alternar o controle Data Terminal Ready (DTR)
linha antes de iniciar o modem chat. Normalmente, o driver serial DTR aumenta quando um processo abre um dispositivo para informar o modem conectado que alguém quer falar com ele. A *dtr-toggle* recurso, então, cai DTR, espera um mo-
mento, e levanta-lo novamente. Muitos modems podem ser configurados para reagir a uma queda de DTR tirando o fone do gancho, entrar
estado de comando ou redefinindo-se.[98]

UUCP sobre o TCP

Por mais absurdo que possa parecer, através do UUCP para transferir dados sobre TCP não é uma péssima idéia, principalmente

quando transferência

anel de grandes quantidades de dados, tais como notícias Usenet. Em links baseados em TCP, a notícia é geralmente de intercâmbio através da
NNTP protocolo, através do qual os artigos são solicitados e enviados individualmente, sem compressão ou qualquer outro otimização. Embora adequado para grandes sites com vários newsfeeds simultâneos, esta técnica é muito unfa-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

pareciam favoráveis para sites pequenos que recebem as suas notícias através de uma conexão relativamente lenta, como ISDN. Estes sites
geralmente querem combinar as qualidades de TCP com as vantagens de enviar notícias em grandes lotes, que podem ser comprimido e, assim, transferida com sobrecarga muito baixa. Uma maneira comum de transferir esses lotes é usar
O UUCP sobre o TCP.

Em *sys*, Você deve especificar um sistema a ser chamado via TCP como este:

98 Alguns modems não parece gostar muito desta e, ocasionalmente travar.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
sistema         GMU
endereço        news.groucho.edu
tempo           Qualquer
porto           tcp-conn
chat            ogin: palavra vstout: Clouseau
```

A `endereço` comando fornece o endereço IP do host ou nome de domínio totalmente qualificado. O correspondente *porto* entrada seria:

```
porto           tcp-conn
tipo            tcp
serviço         540
```

Os estados de entrada que uma conexão TCP deve ser usado quando um *sys* referências entrada *tcp-conn*, E que `uucico` deve tentar se conectar à rede TCP porta 540 no host remoto. Este é o número da porta padrão do serviço de UUCP. Em vez do número da porta, você também pode dar um nome simbólico para o porto `serviço` comando. O número da porta correspondente a esse nome será procurado no */ Etc / services*. O nome comum para o UUCP serviço é *uucpd*.

Usando uma conexão direta

Suponha que você use uma linha directa para ligar o seu sistema *vstout* para *minúsculo*. Assim como no caso do modem, você tem que escrever uma entrada no sistema *sys* arquivo. A `porto` comando identifica a porta serial *minúsculo* está ligado a:

```
sistema         minúsculo
tempo           Qualquer
porto           direct1
velocidade      38400
chat            ogin: palavra Cathcart: Catch22
```

Na *porto* arquivo, você tem que descrever a porta serial para a conexão direta. A *discador* entrada não é necessário ser- porque não há necessidade de marcação:

```
porto           direct1
tipo            directo
velocidade      38400
dispositivo         / Dev/ttyS1
```

Controlando o acesso aos recursos UUCP

O UUCP é um sistema bastante flexível. Com essa flexibilidade é uma necessidade de cuidado controlar o acesso a seus recursos para evitar abusos, seja intencional ou acidental. As principais características de interesse para a administração UUCP Tor é um comando remoto, transferência de arquivos e de encaminhamento. Taylor UUCP fornece um meio de limitar o liberdade que hosts remotos UUCP ter no exercício de cada um desses recursos. Com a cuidadosa selecção de permis- sões, o administrador UUCP pode garantir que a segurança do hospedeiro é preservado.

Execução do Comando

UUCP é tarefa de copiar arquivos de um sistema para outro e para solicitar a execução de certos comandos no controle remoto hosts. Claro, você como administrador gostaria de controlar o que você concede direitos de outros sistemas - que permita -los para executar qualquer comando que escolher no seu sistema não é definitivamente uma boa idéia.

Por padrão, os comandos só Taylor UUCP permite que outros sistemas para executar em sua máquina são `rmail` e `rnews`, Que são comumente usados para troca de e-mail e Usenet News sobre o UUCP. Para alterar o conjunto de com- mandos para um determinado sistema, você pode usar o *comandos* palavra-chave na *sys* arquivo. Da mesma forma, você pode querer limitar o caminho de busca para apenas os diretórios que contém os comandos permitidos. Você pode alterar o caminho de pesquisa permitido para um host remoto com o *comando caminho* declaração. Por exemplo, você pode querer permitir que o sistema *pablo* para executar o `bsmtp` comando, além de `rmail` e `rnews`:[99]

```
sistema pablo ...
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

99 `bsmtp` é usado para entregar e-mails com SMTP lote.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
comandos        rnews rmail bsmtp
```

Transferência de Arquivos

Taylor UUCP também permite transferências afinar arquivo em grande detalhe. Em um extremo, você pode desabilitar transferências de e para um determinado sistema. Basta definir *pedido* para *não*, Eo sistema remoto não será capaz de recuperar qualquer arquivos de seu sistema ou enviá-lo todos os arquivos. Da mesma forma, você pode proibir que seus usuários transfiram arquivos ou de um sistema, definindo *transferência* para *não*. Por padrão, os usuários em ambos os locais e do sistema remoto é permitido upload e download de arquivos.

Além disso, você pode configurar os diretórios que os arquivos podem ser copiados de e para. Normalmente você vai querer restringir o acesso de sistemas remotos a uma hierarquia de diretório único, mas ainda permitir que seus usuários enviem arquivos seu diretório home. Geralmente, os usuários remotos estão autorizados a receber somente os arquivos do diretório UUCP público */ Var / spool / uucppublic*. Este é o local tradicional para tornar os arquivos acessíveis ao público, muito parecido com os servidores FTP na Internet.[100]

Taylor UUCP oferece quatro diferentes comandos para configurar os diretórios para enviar e receber arquivos. São eles: `local-send`, Que especifica a lista de diretórios de um usuário pode pedir o UUCP para enviar arquivos de; `Local-receber`, Que dá a lista de diretórios, um usuário pode pedir para receber arquivos e `remoto envia` e `remoto receber`, Que fazem o análogo para pedidos a partir de um sistema externo. Considere o seguinte exemplo:

```
sistema         pablo
...
local-send      / Home / ~
local de recebimento    / Home / ~ / receber
remoto envia    ~! ~ / Entrada! ~ / Receber
remoto receber  ~ / Incoming
```

A `local-send` comando permite aos usuários do seu host para enviar os arquivos abaixo */ Home* e do público UUCP diretório *pablo*. A `local de recebimento` comando lhes permite receber arquivos quer para o mundo gravável *receber* diretório no *uucppublic*, Ou qualquer diretório graváveis abaixo */ Home*. A `remoto envia` directiva permite *pablo* para solicitar os arquivos de */ Var / spool / uucppublic*, Exceto para os arquivos da *entrada* e *receber* diretórios. Este é um sinal para `uucico` precedendo os nomes de diretório com pontos de exclamação. Por fim, o última linha permite *pablo* para enviar arquivos para *entrada*.

Um dos principais problemas com as transferências de arquivos através do UUCP é que recebe apenas os arquivos para pastas que estão no mundo gravável. Isto pode levar alguns usuários a montar armadilhas para outros usuários. No entanto, não há maneira de escapar desse problem fora de desativar as transferências de arquivos UUCP completamente.

Encaminhamento

UUCP fornece um mecanismo para que outros sistemas, executar transferências de arquivos em seu nome. Por exemplo, suponha o sistema tem `uucp` acesso a um sistema chamado *SECI*, Mas não para outro sistema chamado *uchile*. Isso permite que você fazer *SECI* recuperar um arquivo de *uchile* para si e para enviá-lo ao seu sistema. O seguinte comando irá atingir isso:

```
$ uucp -r SECI! uchile! ~ / find --ls.gz uchile.files.gz /
```

Esta técnica de passar um trabalho através de vários sistemas é chamado *encaminhamento*. Em seu sistema UUCP próprios, você gostaria de limitar o serviço de encaminhamento para alguns servidores da sua confiança para não correr até uma conta de telefone horrendo, fazendo o download da versão mais recente fonte X11R6 para eles.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Por padrão, Taylor UUCP proíbe envio completamente. Para habilitar o encaminhamento para um determinado sistema, você pode usar o `frente` comando. Este comando especifica uma lista de sites o sistema pode pedir-lhe para a frente empregos de e para. Por exemplo, o administrador de UUCP *SECI* teria que adicionar as seguintes linhas para o *sys* arquivo para permitir *pablo* para solicitar os arquivos de *uchile*:

```
####################
```

100 Você pode usar um til (~Character) para se referir ao diretório UUCP público, mas apenas em arquivos de configuração do UUCP; fora dele normalmente trans-
lates para o diretório home do usuário.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# Pablo
sistema         pablo
...
frente          uchile
####################
# Uchile
sistema         uchile
...
frente a        pablo
```

A *frente a* entrada para *uchile* é necessário para que todos os arquivos devolvidos por ela são realmente passados para *pablo*. Ou-Erwise UUCP iria soltá-los. Essa entrada usa uma variação do `frente` comando que permite *uchile* para enviar arquivos somente para *pablo* através *SECI*, E não o contrário.

Que permitem a transmissão a qualquer sistema, use a palavra-chave *QUALQUER* (Letras maiúsculas necessárias).

Configurar o Seu Sistema de discagem

Se você quiser configurar seu site para discar, você tem que permitir logins na sua porta serial e personalizar algumas arquivos de sistema para prestar contas UUCP, que iremos cobrir nesta seção.

Fornecer Contas UUCP

Para começar, você tem que configurar contas de usuário que permitem que sites remotos de log em seu sistema e estabelecer uma UUCP conexão. Geralmente, você irá fornecer um nome de login separado para cada sistema que as pesquisas de você. Ao configurar uma conta para o sistema *pablo*, Você pode dar a ele o nome de usuário *Upablo*. Não existe uma política imposta em nomes de login; eles podem ser qualquer coisa, mas será conveniente para você, se o nome de login é facilmente relacionado com o controle remoto nome do host.

Para sistemas com ligação através da porta serial, você geralmente tem que adicionar essas contas para a senha do sistema arquivo */ Etc / passwd*. É uma boa prática de colocar todos os logins UUCP em um grupo especial, como *uuguest*. A conta de diretório home deve ser definido como o diretório de spool público */ Var / spool / uucppublic*; Seu shell de login deve ser `uucico`.

Para servir os sistemas UUCP que ligam para o seu site através de TCP, você tem que configurar `inetd` para lidar com entrada con-nections na *uucp* porta, acrescentando a seguinte linha */ Etc / inetd.conf*:[101]

```
uucp   stream  tcp   nowait  root  / Usr / sbin / tcpd      / Usr / lib / uucp /
uucico-l
```

A *-L* opção faz com que `uucico` realizar a sua autorização login. Ele pede um login e uma senha assim como o padrão `login` programa, mas confia em seu banco de dados de senha pessoal, em vez de */ Etc / passwd*. Este arquivo de senhas particulares é nomeado */ Uucp / etc / passwd* e contém pares de nomes e senhas de login:

```
Upablo  IslaNegra
Ulorca  co'rdoba
```

Este arquivo deve ser propriedade de *uucp* e ter permissões de 600.

Será que este som de banco de dados como uma idéia tão boa que você gostaria de usá-lo em logins normais de série, também?

Bem, em alguns casos, você pode. O que você precisa é de um `getty` programa que você pode dizer para invocar `uucico` em vez de `/ Bin / login` para seus usuários UUCP.[102] A invocação de `uucico` ficaria assim:

```
/ Usr / lib / uucp / uucico-l-u      usuário
```

A *-U* opção diz-lhe para usar o nome de usuário especificado em vez de perguntar para ele.[103]

Para proteger seus usuários UUCP de chamadores que poderia dar um nome falso sistema snarf e toda a sua correspondência, você deve adicionar `chamado de login` comandos para cada entrada do sistema no *sys* arquivo. Isso é descrito na próxima seção.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

101 Note-se que `tcpd` normalmente tem o modo 700, para que você deve chamá-lo como usuário *root*, Não *uucp*.`tcpd` é discutido em detalhes no Capítulo 12, *Rede Características importantes*.

102 Gert Doering `mgetty` é como uma besta. Ele roda em uma variedade de plataformas, incluindo SCO Unix, AIX, SunOS, HP-UX e Linux.

103 Esta opção não está presente na versão 1.04.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Protegendo-se Contra Trapaceiros

Um grande problema com o UUCP é que o sistema de chamada pode mentir sobre seu nome, ele anuncia o seu nome ao

chamado
sistema após o logon, mas o servidor não tem nenhuma maneira de verificar isso. Assim, um atacante pode entrar no seu ou UUCP sua conta própria, fingir ser outra pessoa, e pegar e-mails que outro site. Isto é particularmente trou-
blesome se você oferecer login via UUCP anônimo, onde a senha é tornada pública.

Você *deve* precaver contra esse tipo de impostor. A cura para esta doença é exigir que cada sistema para usar um particu-
nome de login lar, especificando um *chamado de login* em *sys*. A entrada do sistema de amostra pode ser parecido com este:

```
sistema         pablo
... opções habituais ...
chamado de      Upablo
login
```

O resultado é que sempre que um sistema se conecta e finge que é *pablo*,`uucico` verifica se tem registado no
como *Upablo*. Se não tiver, o sistema de chamada é voltada para baixo, ea conexão é descartado. Você deve torná-lo um hábito de adicionar o `chamado de login` comando para cada entrada no sistema você adiciona ao seu *sys* arquivo. É importante que
você faz isso para *todos* sistemas em seu `sys` arquivo, independentemente de eles nunca vão chamar o seu site ou não. Para aqueles
sites que nunca te chamam, você provavelmente deve definir *chamado de login* por um nome de usuário totalmente falsos, como *neverlog-*
pecado.

Seja Paranoid: Verifica chamada seqüência

Outra maneira de se defender e detectar impostores é usar `sequência de controlos de chamada`. Estes ajudam a

proteger
contra intrusos que de alguma forma conseguem descobrir a senha com que você entrar no seu sistema UUCP.

Quando as verificações seqüência usando a chamada, ambas as máquinas acompanhar o número de conexões estabelecidas até

agora. A
contador é incrementado a cada conexão. Após o login, o chamador envia seu número de seqüência de chamadas, e os receptor verifica-lo contra o seu próprio número. Se eles não corresponderem, a tentativa de conexão será rejeitada. Se a inicial número é escolhido aleatoriamente, os atacantes terão um tempo difícil adivinhar o número de seqüência correta chamada.

Mas verifica chamada seqüência fazer mais por você. Mesmo se uma pessoa muito inteligente deverá detectar a sua seqüência de

chamada
número, bem como sua senha, você vai descobrir. Quando o atacante chama seu feed UUCP e rouba o seu
e-mail, isso vai aumentar o número de seqüência de feeds chamar um por um. A próxima vez *você* chamar o seu feed e tentar fazer o login,
o controle remoto `uucico` irá recusar-lhe, porque os números não correspondem mais!

Se você tiver habilitado cheques chamada seqüência, você deve verificar seus arquivos de log regularmente para mensagens de

erro que dica
a possíveis ataques. Se o sistema rejeita o número de seqüência de chamar o sistema oferece, chamando, `uucico` vai colocar um
mensagem no arquivo de log dizendo algo como: "fora da seqüência chamada rejeitada." Se o seu sistema é rejeitado por sua alimentação, porque os números de seqüência estão fora de sincronia, ele vai colocar uma mensagem no arquivo de log dizendo, "Aperto de mão
falhou (RBADSEQ). "

Para habilitar chamada verifica seqüência, adicione o seguinte comando para a entrada do sistema:

```
# Permitir um controlo chamada seqüência
seqüência       verdade
```

Além disso, você tem que criar o arquivo que contém o número de seqüência em si. Taylor UUCP mantém a seqüência de número em um arquivo chamado . *Sequence* no diretório de spool do site remoto. É *deve* ser propriedade de *uucp* e deve ser

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Modo de 600 (ou seja, legível e gravável apenas pelo *uucp*). É melhor para inicializar este arquivo com uma extensão arbitrária, já
acordados valor inicial. Uma maneira simples de criar este arquivo é:

```
#  cd / spool / var / uucp / pablo
#  echo 94316>. seqüência
#  chmod 600. Sequence
#  chown uucp.uucp. Sequence
```

Claro, o site remoto para permitir um controlo chamada seqüência tão bem e começar usando exatamente a mesma se-
número de seqüência como você.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Anónimo UUCP

Se você deseja fornecer acesso UUCP anônimos ao seu sistema, você primeiro tem que configurar uma conta especial para ele como descrito anteriormente. Uma prática comum é dar a conta anônima um login e uma senha de *uucp*.

Além disso, você tem que ajustar algumas das opções de segurança para sistemas desconhecidos. Por exemplo, você pode querer proibi-los de executar os comandos em seu sistema. No entanto, você não pode definir esses parâmetros em uma *sys* entrada de arquivo, porque o `sistema` comando requer o nome do sistema, que você não tem. Taylor UUCP resolve este dilema através da `desconhecido` comando. `desconhecido` pode ser usado na *config* arquivo para especificar qualquer
de comando que normalmente pode aparecer em uma entrada do sistema:

```
desconhecido    remoto receber ~ / incoming
desconhecido    remoto envia ~ / pub
desconhecido    none max-remoto-debug
desconhecido    comando caminho / usr / lib / uucp / anon-bin
desconhecido    comandos rmail
```

Isto irá restringir sistemas desconhecidos para baixar arquivos abaixo do *pub* diretório e fazer upload de arquivos para o *entrada* diretório abaixo */ Var / spool / uucppublic*. A próxima linha vai fazer `uucico` ignorar as solicitações do sistema remoto para ativar a depuração no local. As últimas duas linhas permitem a execução de sistemas desconhecidos `rmail`, Mas
o caminho do comando especificado faz `uucico` olhar para o `rmail` comando em um diretório privado chamado *anon bin* apenas. Esta restrição permite que você fornecer algumas especiais `rmail` que, por exemplo, encaminha tudo para a superusuário para exame. Isso permite que usuários anônimos chegar ao mantenedor do sistema, mas ao mesmo tempo tempo os impede de injetar um novo email para outros sites.

Para habilitar o UUCP anônimo, você deve especificar pelo menos um *desconhecido* declaração em *config*. Caso contrário

`uucico`
vai rejeitar todos os sistemas desconhecidos.

Protocolos UUCP de Baixo Nível

Para negociar o controle de sessão e transferência de arquivos com o ponto remoto, `uucico` usa um conjunto de mensagens

padronizadas.
Isso é muitas vezes referido como o `protocolo de alto nível`. Durante a fase de inicialização e desligamento da fase estes são simplesmente enviado por meio de cordas. No entanto, durante a fase de transferência real, um protocolo de baixo nível adicional
que é mais transparente para os níveis mais elevados é empregado. Este protocolo oferece alguns benefícios adicionais, tais como
que permitam o controlo de erro nos dados enviados através de links não confiáveis.

Protocolo Geral

UUCP é usado em diferentes tipos de conexões, tais como linhas seriais, TCP, ou às vezes até X.25, é vantajoso para o transporte de UUCP dentro de protocolos projetado especificamente para o protocolo de rede subjacente. Em Além disso, várias implementações de UUCP introduziram diferentes protocolos que fazer praticamente a mesma coisa.

Os protocolos podem ser divididos em duas categorias: `streaming` e `pacote` protocolos. Protocolos de streaming variedade de transferência de um arquivo como um todo, possivelmente, uma soma de computação sobre ele. Isto é quase livre de sobrecarga, mas
requer uma conexão confiável, pois qualquer erro fará com que todo o arquivo para ser retransmitido. Estes protocolos são comumente usado em conexões TCP, mas não são adequados para uso em linhas telefônicas. Apesar de mo-moderna dems fazer um bom trabalho de correção de erro, eles não são perfeitos, nem há qualquer identificação de erro entre o computador e do modem.

Por outro lado, os protocolos de pacotes orientada a dividir o arquivo em vários pedaços de tamanho igual. Cada pacote é enviados e recebidos, separadamente, um checksum é calculado, e uma confirmação é retornada para o remetente. Para torná-las mais eficientes, protocolos de janela deslizante ter sido inventado, o que permite um número limitado (a janela) de confirmações pendentes a qualquer momento. Isso reduz muito a quantidade de tempo `uucico` tem que

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

esperar durante uma transmissão. Ainda assim, o overhead relativamente grande em relação a um protocolo de streaming faz pacote
protocolos ineficientes para o uso do TCP, mas ideal para linhas telefônicas.

A largura do caminho de dados também faz a diferença. Às vezes, o envio de caracteres de 8 bits em uma conexão serial
É impossível, por exemplo, a conexão poderá passar por um servidor de terminal burro que descasca o oitavo bit.
Quando você transmitir caracteres de 8 bits em uma conexão de 7 bits, eles têm de ser cotadas na transmissão. Na pior,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

scenerio caso, citando dobra a quantidade de dados a ser transmitido, embora a compressão feita pelo hardware pode compensar. Linhas que podem transmitir caracteres arbitrários de 8 bits são chamados geralmente *8-bit limpo*. Este é o caso para todas as conexões TCP, bem como para a maioria das conexões de modem.

Taylor UUCP 1,06 suporta uma ampla variedade de protocolos de UUCP. Os mais comuns são:

g

Este é o protocolo mais comum e deve ser entendido por praticamente todos os `uucico`s. Ele faz completa verificação de erros e, portanto, bem adequado para ligações telefónicas ruidosos. *g* requer um 8-bit limpo conexão. É um protocolo packet-oriented, que utiliza uma técnica de janela deslizante.

i

Este é um protocolo de pacotes bidirecional, que pode enviar e receber arquivos, ao mesmo tempo. Ela exige uma full-duplex de conexão e um 8-bit caminho de dados limpo. Hoje é entendida por Taylor UUCP só.

t

Este protocolo é destinado ao uso em uma conexão TCP ou outras redes verdadeiramente livre de erros. Usa-pack ets de 1.024 bytes e requer uma conexão de 8 bits limpos.

e

Isso deve fazer basicamente o mesmo que *t*. A principal diferença é que *e* é um protocolo de streaming e é assim adequado apenas para conexões de rede confiável.

f

Isto é destinado para uso com conexões confiáveis X.25. É um protocolo de transmissão e espera um 7-bit caminho de dados. caracteres de 8 bits são citados, o que pode torná-lo muito ineficiente.

G

Este é o System V Release 4 versão do *g* protocolo. Também é entendido por outras versões do UUCP.

um

Este protocolo é semelhante ao ZMODEM. É necessária uma conexão de 8 bits, mas cita características de controle determina-
tros como XON e XOFF.

Ajustando o Protocolo de Transmissão

Todos os protocolos permitem alguma variação no tamanho dos pacotes, timeouts, etc Geralmente, os padrões de trabalhar bem sob stan-
dard circunstâncias, mas pode não ser ideal para a sua situação. A *g* protocolo, por exemplo, usa tamanhos de janela 1-7, e tamanhos de pacotes em potências de 2 variando de 64 a 4096. Se a linha telefônica é normalmente tão barulhento que ele cai mais de 5 por cento de todos os pacotes, você provavelmente deve diminuir o tamanho do pacote e diminuir o janela. Por outro lado, nas linhas de telefone muito bom overhead do protocolo de envio de avisos para cada 128 bytes pode revelar-se inútil, então você pode aumentar o tamanho do pacote para 512 ou mesmo 1024. A maioria dos binários incluídos no padrão Linux distribuições para um tamanho de janela de 7 e pacotes de 128 bytes.

Taylor UUCP permite parâmetros de sintonia com o `protocolo de parâmetro` comando na *sys* arquivo. Para in-postura, para definir o *g* tamanho do protocolo de pacotes para 512 quando se fala de *pablo*, Você tem que adicionar:

```
sistema         pablo
...
g-protocolo parâmetro pacotes de tamanho  512
```

Os parâmetros ajustáveis e seus nomes variam de protocolo para protocolo. Para obter uma lista completa delas, referem-se ao documentação inclusa na fonte UUCP Taylor.

Seleção de protocolos específicos

Não execução de cada `uucico` fala e entende cada protocolo, portanto, durante o handshake inicial fase, ambos os processos têm que concordar com um comum. O mestre `uucico` oferece o escravo de uma lista de suporte

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

protocolos através do envio de P*protlist*, Da qual o escravo pode escolher uma.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Com base no tipo de porta usada (modem, TCP, ou directa), `uucico` irão compor uma lista padrão de protocolos. Para modem e conexões diretas, esta lista inclui normalmente *i*,*um*,*g*,*G*E *j*. Para conexões TCP, a lista é *t*,*e*,*i*, *um*,*g*,*G*,*j*E *f*. Você pode substituir essa lista padrão com o `protocolos` comando, que podem ser especificados em um entrada do sistema, bem como uma porta de entrada. Por exemplo, você pode editar o *porto* entrada do arquivo para a porta do modem, como
isso:

```
porto           serial1
...
protocolos      IgG
```

Isto requer nenhuma conexão de entrada ou saída através desta porta para usar *i*,*g*Ou *G*. Se o sistema remoto não apoiar qualquer dessas, a conversa irá falhar.

Solução de problemas

Esta seção descreve o que pode dar errado com sua conexão UUCP e faz sugestões para corrigir a localização o erro. Embora estes problemas são encontrados em uma base regular, há muito mais que pode dar errado do que aquilo que temos listados.

Se você tiver um problema, habilitar a depuração com *-XALL*, E dê uma olhada na saída do *Depurar* no diretório de spool. O arquivo deverá ajudá-lo a reconhecer rapidamente o problema. Muitas vezes é útil para ligar alto-falante do modem quando ele não ligar. Com modems Hayes-compatível, você pode ativar o orador, acrescentando `ATL1M1 OK` para o modem de bate-papo na *dial* arquivo.

O primeiro cheque deve ser sempre se todas as permissões do arquivo estão definidos corretamente. `uucico` deve ser setuid *uucp*,
e todos os ficheiros */ Usr / lib / uucp*,*/ Var / spool / uucp*E */ Var / spool / uucppublic* devem pertencer ao *uucp*. Há também alguns arquivos ocultos no diretório de spool, que deve ser de propriedade da *uucp* também.[104]

Quando você tem certeza você tem as permissões de todos os arquivos corretamente configurado, e você ainda estiver enfrentando problemas, você
pode então começar a receber mensagens de erro mais literalmente. Vamos agora olhar para alguns dos erros mais comuns e problemas.

Mantém uucico Dizer "Wrong Time to Call"

Isso provavelmente significa que na entrada do sistema em *sys*, Você não especificar um `tempo` comando que detalhes quando a sistema remoto pode ser chamado, ou você deu uma que realmente proíbe chamado no momento atual. Se nenhum agendamento chamada
é dado, `uucico` assume que o sistema nunca pode ser chamado.

uucico reclama que o site já está bloqueado

Isso significa que `uucico` detecta um arquivo de bloqueio para o sistema remoto em */ Var / spool / uucp*. O arquivo de bloqueio pode ser de
uma chamada anterior para o sistema que caiu ou foi morto. Outra explicação possível é que há outra `uucico` processo de audiência em torno de que está tentando marcar o sistema remoto e ficou preso em um script de chat, ou estagnado por algum outro motivo.

Para corrigir este erro, matar todos os `uucico` processos abertos para o site com um sinal de desligar e remover todos os arquivos de bloqueio
que deixaram cerca de mentir.

Você pode se conectar ao site remoto, mas o script falhar Chat

Olha o texto que você recebe do site remoto. Se ele é distorcido, você pode ter um problema de velocidade relacionados. Ou-Do contrário, confirma que realmente concorda com o que o script de bate-papo espera. Lembre-se, o bate-papo começa com um script

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

esperar string. Se você receber o aviso de login e enviar seu nome, mas nunca chegar a senha, insira alguns atrasos, antes de enviá-lo, ou mesmo entre as letras. Você pode ser muito rápido para o seu modem.

104 Ou seja, arquivos com nomes que começam com um ponto. Esses arquivos normalmente não são exibidos pelo `ls` comando.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Seu modem não disca

Se o seu modem não indica que a linha DTR foi levantada quando `uucico` chama, você pode não ter
dado o direito de dispositivo `uucico`. Se o modem reconhece DTR, verifique com um programa de terminal que você pode escrever para o modem. Se isso funcionar, ligue ecoando \ *E* no início do modem chat. Se o modem não
echo seus comandos durante o bate-papo modem, verifique se a velocidade da linha é muito alta ou baixa. Se você ver o eco, verifique se você tiver desativado respostas modem ou defini-los como códigos numéricos. Verifique se o script de chat em si é correta. Lembre-se que você tem que escrever duas barras invertidas para enviar uma para o modem.

Seu modem tenta discar, mas não sai

Inserir um atraso para o número de telefone, especialmente se você tiver que discar uma seqüência especial para obter uma linha

externa
a partir de uma rede de telefonia da empresa. Verifique se você está usando o tipo de discagem correta, já que algumas redes de telefonia
suportam apenas um tipo de marcação. Além disso, verifique o número de telefone para se certificar de que está correto.

Autenticação for bem sucedida, mas a falha de handshake

Bem, pode haver uma série de problemas nesta situação. A saída no arquivo de log deve dizer-lhe muito. Olhe
quais os protocolos que o site oferece remoto (que envia uma string P*protlist* durante o handshake). Para o aperto de mão para sucesso, ambas as extremidades devem suportar pelo menos um protocolo comum, de modo a verificar que eles fazem.

Se o sistema remoto envia `RLCK`, Há uma lockfile obsoleto para você no sistema remoto já estiver conectado ao
sistema remoto em uma linha diferente. Caso contrário, pergunte ao administrador do sistema remoto para remover o arquivo.

Se o sistema remoto envia `RBADSEQ`, Tem cheques conversa contagem habilitado para você, mas os números não
partida. Se ele envia `RLOGIN`, Você não era permitido fazer logon no âmbito deste ID.

Os arquivos de log e depuração

Ao compilar o pacote UUCP usar Taylor estilo de log, você tem apenas três arquivos de log global, que
residir no diretório de spool. O arquivo de log principal é chamado *Entrar* e contém todas as informações sobre estabelecidas ligações e arquivos transferidos. Um excerto típico é assim (depois de uma reformatação pouco para torná-lo apto a página):

```
uucico pablo - (1994-05-28 17:15:01.66 539) pablo sistema de chamada (porta
cua3)
uucico pablo - (1994-05-28 17:15:39.25 539) Entrar com êxito
uucico pablo - (1994-05-28 17:15:39.90 539) Handshake sucesso
               (Tamanho "g" packet protocol 1024 janela 7)
postmaster uucico pablo (1994-05-28 17:15:43.65 539) Recebendo D.pabloB04aj
postmaster uucico pablo (1994-05-28 17:15:46.51 539) Recebendo X.pabloX04ai
postmaster uucico pablo (1994-05-28 17:15:48.91 539) Recebendo D.pabloB04at
postmaster uucico pablo (1994-05-28 17:15:51.52 539) Recebendo X.pabloX04as
postmaster uucico pablo (1994-05-28 17:15:54.01 539) D.pabloB04c2 Receber
postmaster uucico pablo (1994-05-28 17:15:57.17 539) Recebendo X.pabloX04c1
uucico pablo - (1994/05/28 17:15:59.05 539) pacotes 'g', Protocolo: enviou 15,
                ressentem 0, recebeu 32
uucico pablo - (1994/05/28 17:16:02.50 539) Call completo (26 segundos)
postmaster pablo uuxqt (1994-05-28 17:16:11.41 546) Executora X.pabloX04ai
               (Okir rmail)
postmaster pablo uuxqt (1994-05-28 17:16:13.30 546) Executora X.pabloX04as
               (Okir rmail)
postmaster pablo uuxqt (1994-05-28 17:16:13.51 546) Executora X.pabloX04c1
               (Okir rmail)
```

O próximo arquivo de log é importante *Estatísticas*, Que enumera as estatísticas de transferência de arquivo. A seção de

Estatísticas correspondente ao
transferência acima se parece com isso (mais uma vez, as linhas foram divididas para caber na página):

```
pablo postmaster (1994/05/28 17:15:44.78)
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
                    recebeu 1.714 bytes em 1,802 segundo (951 bytes /)
pablo postmaster (1994/05/28 17:15:46.66)
                    recebeu 57 bytes em 0,634 segundo (89 bytes /)
pablo postmaster (1994/05/28 17:15:49.91)
                    recebeu 1.898 bytes em 1,599 segundo (1186 bytes /)
pablo postmaster (1994/05/28 17:15:51.67)
                    recebeu 65 bytes em 0,555 segundo (117 bytes /)
pablo postmaster (1994/05/28 17:15:55.71)
                    recebeu 3.217 bytes em 2,254 segundo (1427 bytes /)
pablo postmaster (1994/05/28 17:15:57.31)
                    recebeu 65 bytes em 0,590 segundo (110 bytes /)
```

O terceiro arquivo é *Depurar*. A informação de depuração está escrito aqui. Se você usar a depuração, certifique-se o arquivo tem
modo de proteção 600. Dependendo do modo de depuração que você selecionar, ele pode conter o login ea senha que você usa para se conectar ao sistema remoto.

Se você tem algumas ferramentas que esperam em torno de seus arquivos de log a ser no formato tradicional usado por HDB-compatíveis
implementações UUCP, você também pode compilar Taylor para produzir HDB UUCP estilo de logs. Isto é simplesmente uma questão
de permitir uma opção em tempo de compilação em *config.h*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 17 - Correio Eletrônico

Transporte de correio eletrônico tem sido um dos usos mais importantes da rede desde as primeiras redes foram planejado. Email começou como um simples serviço que copiou um arquivo de uma máquina para outra e anexa-lo ao destinatário *caixa de correio* arquivo. O conceito permanece o mesmo, apesar de uma rede em constante crescimento, com seu complexo de roteamento
requisitos e sua carga cada vez maior de mensagens, fez um esquema mais elaborado, necessário.

Vários padrões de troca de correio foram concebidas. Sites na Internet aderir a uma definidos na RFC-822, complementado por algumas RFCs que descrevem uma forma independente de máquina de transferência de apenas cerca de *nada*, Inclu-
ção de gráficos, arquivos de som e conjuntos de caracteres especiais, por e-mail.[105] CCITT definiu outro X.400, padrão. É ainda é utilizado em algumas grandes ambientes corporativos e governamentais, mas está sendo progressivamente aposentado.

Um grande número de programas de transporte de correio têm sido implementadas para sistemas Unix. Um dos mais conhecidos é
`sendmail`, Que foi desenvolvido por Eric Allman na Universidade da Califórnia em Berkeley. Eric Allman agora oferece `sendmail` através de um empreendimento comercial, mas o programa continua a ser o software livre. `sendmail` é fornecido
como o agente de correio padrão em algumas distribuições Linux. Nós descrevemos `sendmail` configuração no Capítulo 18, *Sendmail*.

Linux também usa `Exim`, Escrita por Philip Hazel da Universidade de Cambridge. Nós descrevemos `Exim` configuração no Capítulo 19, *Obter Exim Funcionando*.

Em comparação com `sendmail`,`Exim` é bastante jovem. Para a grande maioria dos sites com as exigências e-mail, a sua capaci-
dades estão muito perto.

Ambos `Exim` e `sendmail` suporte um conjunto de arquivos de configuração que tem que ser personalizado para o seu sistema. Além das informações que são necessárias para tornar o subsistema de correio executar (como o nome da máquina local), há muitos parâmetros que podem ser sintonizadas. `sendmail`'S principal arquivo de configuração é muito difícil de entender à primeira vista.
É como se o seu gato tenha tirado um cochilo no teclado com a tecla shift pressionada. `Exim` arquivos de configuração são mais estruturada e mais fácil de entender do que `sendmail`'S. `Exim`No entanto, não fornece suporte direto para UUCP e trata apenas endereços de domínio. mais, que hoje não é tão grande limitação, como já poderia ter sido sites permanecer dentro `Exim`'S limitações. No entanto, para a maioria dos sites, o trabalho necessário na criação de qualquer um deles é
praticamente o mesmo.

Neste capítulo, vamos lidar com o e-mail é e quais as questões que os administradores têm de lidar. Capítulo 18 e Capítulo 19 fornece instruções sobre como configurar `sendmail` e `Exim` e pela primeira vez. As informações incluídas-informação deve ajudar pequenos sites em funcionamento, mas existem várias opções e você pode passar muitos happy hour na frente do seu computador configurando o fanciest recursos.

Para o fim deste capítulo, brevemente abordar a criação de `olmo`, O agente de correio muito comum no Unix muitos sistemas similares, incluindo o Linux.

Para mais informações sobre questões específicas de correio eletrônico em Linux, consulte o correio electrónico HOWTO por Aznar Guylhem,[106] que é colocada comp.os.linux.answers regularmente. A distribuição fonte do `olmo`,`Exim`E `sendmail` também contêm vasta documentação que deve responder a mais perguntas sobre a configuração los, e nós fornecemos as referências a esta documentação em seus respectivos capítulos. Se você precisa em geral formação em e-mail, um número de RFCs lidar com este tema. Eles estão listados na bibliografia ao final do livro.

O que é uma mensagem de correio?

Uma mensagem de correio geralmente consiste de um corpo de mensagem, que é o texto da mensagem e, em especial admi-tiva de dados especificando destinatários, meio de transporte, etc, gosta do que vê quando se olha para uma carta de física envelope

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

105 Leia RFC-1437, se você não acredita que esta declaração!
106 Guylhem pode ser alcançado em *guylhem@danmark.linux.eu.org*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Estes dados administrativos se divide em duas categorias. Na primeira categoria é qualquer dado que é específico para o transporte
médio, como o endereço do remetente e do destinatário. Por isso, é chamado de *envelope*. Pode ser transformado pelo software de transporte como a mensagem é passada adiante.

A segunda variedade é todos os dados necessários para lidar com a mensagem de correio, que não é específico para o transporte mecanismo, como a linha de assunto da mensagem, uma lista de todos os beneficiários, bem como a data a mensagem foi enviada. Em muitos
redes, tornou-se padrão para preceder esses dados à mensagem de correio, formando o chamado *cabeçalho do e-mail*. É é deslocada do *corpo da mensagem* por uma linha vazia.[107]

A maioria dos softwares de transporte de email no mundo Unix usam um formato de cabeçalho descrito na RFC-822. Sua finalidade original
foi para especificar um padrão para uso na ARPANET, mas desde que ele foi projetado para ser independente de qualquer ambiente, foi facilmente adaptado para outras redes, incluindo muitos baseados em redes de UUCP.

RFC-822 é apenas o mínimo denominador comum, no entanto. normas mais recentes têm sido concebidas para fazer face com as necessidades de crescimento, tais como criptografia de dados, suporte conjunto de caracteres internacionais, e MIME (Multipurpose Inter-
net Mail Extensions, descrito na RFC-1341 e outras RFCs).

Em todas essas normas, o cabeçalho é composto por várias linhas separadas por uma ponta de seqüência-line. A linha é feita por um nome de campo, a partir de uma coluna, eo próprio campo, compensado por uma vírgula e espaço em branco. O formato e semântica de cada campo variar dependendo do nome do campo. Um campo de cabeçalho pode ser continuado através de uma nova linha
Se a próxima linha começa com um caractere espaço em branco como separador. Os campos podem aparecer em qualquer ordem.

Um cabeçalho de correio normal pode ser parecido com este:

```
Return-Path: <ph10@cus.cam.ac.uk>
Recebido: ursa.cus.cam.ac.uk (cusexim@ursa.cus.cam.ac.uk [131.111.8.6])
    por al.animats.net (8.9.3/8.9.3/Debian 8.9.3-6) with ESMTP id WAA04654
    para <terry@animats.net>; Sun, 30 de janeiro de 2000 22:30:01 1100
Recebido: de PH10 (helo = localhost) por ursa.cus.cam.ac.uk com smtp local
    (Exim 3,13 # 1) id 12EsYC-0001eF-00; Sun, 30 de janeiro de 2000 11:29:52 0000
Date: Thu, 30 jan 2000 11:29:52 +0000 (GMT)
De: Philip Hazel <ph10@cus.cam.ac.uk>
Reply-To: Philip Hazel <ph10@cus.cam.ac.uk>
Para: <terry@animats.net> Terry Dawson, Andy Oram <andyo@oreilly.com>
Assunto: Electronic capítulo mail
In-Reply-To: <38921283.A58948F2 @ animats.net>
Message-ID: <Pine.SOL.3.96.1000130111515.5800A-200000@ursa.cus.cam.ac.uk>
```

Normalmente, todos os campos de cabeçalho necessários são gerados pela interface mailer você usa, como `olmo`,`pinheiro`,`mush`Ou
`mailx`. No entanto, alguns são opcionais e podem ser adicionados pelo usuário. `olmo`, Por exemplo, permite que você edite parte
cabeçalho da mensagem. Outros são adicionados pelo software de transporte de correio. Se você olhar para uma caixa de correio local, você
pode ver cada mensagem de correio precedido por uma linha "De" (nota: no cólon). Esta é *não* um cabeçalho RFC-822, tem sido inserido pelo software de e-mail como uma conveniência para os programas de leitura da caixa de correio. Para evitar possíveis trou-
vel com as linhas no corpo da mensagem, que também começa com o procedimento "De", tornou-se padrão para escapar de qualquer
tal ocorrência se precedida por um caractere>.

Esta lista é uma coleção de campos de cabeçalho comuns e seus significados:

`De:`

Este contém o endereço de e-mail do remetente e, possivelmente, o "verdadeiro nome". Um jardim zoológico completo de formatos é
usados aqui.

`Para:`

Esta é uma lista de endereços de e-mail do destinatário. os endereços dos destinatários múltiplas são separadas por uma

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

vírgula.

`Cc:`

Esta é uma lista de endereços de e-mail que receberá "cópias carbono" da mensagem. Vários anúncios destinatário vestidos são separadas por uma vírgula.

[107] Costuma-se acrescentar um *assinatura* ou . *Sig* uma mensagem de correio, geralmente contendo informações sobre o autor, juntamente com uma piada ou uma
lema. É offset da mensagem de correio por uma linha contendo "`-`"Seguido de um espaço

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`Bcc:`

Esta é uma lista de endereços de e-mail que receberá "cópias carbono" da mensagem. A principal diferença ser-
entre um "Cc:" e um "Cco:" é que os endereços listados em um "Cco:" não vai aparecer no cabeçalho do
mensagens de correio entregue a qualquer destinatário. É uma forma de alertar os destinatários que você enviou cópias do
mensagem para outras pessoas sem lhes dizer que os outros são. Vários são os endereços dos destinatários
separadas por uma vírgula.

`Assunto:`

Descreve o conteúdo da mensagem em poucas palavras.

`Data:`

Suprimentos para a data e hora do e-mail foi enviado.

`Responder para:`

Especifica o endereço do remetente quer a resposta do beneficiário dirigida. Isso pode ser útil se você tiver
várias contas, mas quer receber a maior parte do correio apenas no que você usa com mais freqüência. Este
campo é opcional.

`Organização:`

A organização que possui a máquina a partir do qual se origina o e-mail. Se a sua máquina é de propriedade da
você em particular, deixe isso, ou inserir "privado" ou algum disparate completo. Este campo não é de-
descrito por qualquer RFC e é totalmente opcional. Alguns programas de correio apoiá-lo diretamente, muitos não.

`Message-ID:`

Uma seqüência de caracteres gerados pelo transporte de email no sistema de origem. Ele identifica esta mensagem.

`Recebido:`

Todos os sites que os processos de seu e-mail (incluindo as máquinas de remetente e destinatário) insere um campo tão
no cabeçalho, dando o seu nome do site, uma mensagem de identificação, data e hora que recebeu a mensagem, a qual site ele
é, e qual o software de transporte foi utilizado. Estas linhas permitem traçar a via mensagem
teve, e você pode reclamar com a pessoa responsável se algo der errado.

`X-`*qualquer coisa:*

Não há programas relacionados a correio devem reclamar sobre qualquer cabeçalho que começa com `X-`. Ele é usado
para implementar
recursos adicionais que ainda não fizeram isso em um RFC, ou nunca. Por exemplo, já houve uma
muito grande servidor Linux mailing list que permitiu que você especifique qual canal você queria que o e-mail para
ir para a cadeia, adicionando `X-Mn-chave`: seguido do nome do canal.

Como está o correio entregado?

Geralmente, você irá escrever e-mail utilizando uma interface mailer como `e-mail` ou `mailx`, Ou as mais sofisticadas, como `mutt`,`tkrat`Ou `pinheiro`. Estes programas são chamados *os agentes do utilizador e-mail*Ou MUAs. Se você enviar uma mensagem de correio, o
interface de programa, na maioria dos casos, entregá-lo para outro programa para a entrega. Este é o chamado *transporte de correio*
agente, Ou MTA. Na maioria dos sistemas do MTA é utilizado o mesmo tanto para o fornecimento local e remoto, e é geralmente in-
vocados como `/ Usr / sbin / sendmail`, Ou sobre a não-FSSTND sistemas compatíveis como `/ Usr / lib / sendmail`. Em
sistemas UUCP não é incomum ver a entrega de correio manipulados por dois programas distintos: `rmail` para controle remoto entrega de correio e `lmail` para a entrega de correio local.

Local de entrega do correio, é claro, mais do que apenas anexar a mensagem de entrada para a caixa postal do destinatário. Normalmente, o MTA local entende aliasing (criação destinatário endereços locais apontando para outros endereços)
e encaminhamento (redirecionamento de correio de um usuário para algum outro destino). Além disso, as mensagens que não podem ser entregues
deve ser normalmente *saltado*, Ou seja, devolvido ao remetente juntamente com alguma mensagem de erro.

Para entrega remota, o software de transporte utilizado depende da natureza do vínculo. Mail entregues através de uma rede

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

usando TCP / IP utiliza geralmente *Simple Mail Transfer Protocol* (SMTP), que é descrito na RFC-821. SMTP foi concebida para fornecer e-mail diretamente para a máquina do destinatário, negociando a transferência da mensagem com o controle remoto daemon lado de SMTP. Hoje, é prática comum para as organizações estabelecerem anfitriões especiais que aceitar todas as e-mail para os destinatários na organização e acolhimento para que possam administrar a oferta adequada ao destinatário pretendido.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Mail não é normalmente entregue diretamente nas redes de UUCP, mas é encaminhado para o host de destino por um número de sistemas intermediários. Para enviar uma mensagem através de uma ligação UUCP, a MTA que envia normalmente executa
`rmail` sobre o sistema de transmissão usando `uux`, E alimenta a mensagem na entrada padrão.

Desde `uux` é chamado para cada mensagem separadamente, pode produzir uma carga de trabalho considerável em um hub de correio,
bem como a desorganização das filas spool UUCP com centenas de arquivos pequenos tendo uma quantidade desproporcional de de espaço em disco.[108] Alguns MTAs, portanto, permitem que você coletar várias mensagens para um sistema remoto em um único lote
arquivo. O arquivo em lote contém os comandos SMTP que o host local, normalmente, se um problema de SMTP direta ligação foram utilizados. Isso é chamado BSMTP, ou *batched* SMTP. O lote é então levado à `rsmtp` ou `bsmtp`
programa no sistema remoto, que processa a entrada quase como se uma conexão SMTP normal ocorreu.

Endereços de email

Os endereços são compostos de pelo menos duas partes. Uma parte é o nome de um *domínio de correio* que finalmente traduzir para o host do destinatário ou algum servidor que aceita e-mails em nome do destinatário. A outra parte é alguma forma de identificação exclusiva do usuário que pode ser o nome desse usuário, o nome real do usuário no que "Nome.Apelido" formato, ou um alias arbitrário que será traduzida para um usuário ou lista de usuários. Outros mail esquemas de endereçamento, como X.400, use um conjunto mais geral de "atributos" que são usados para procurar host do destinatário
em um servidor de diretório X.500.

Como endereços de e-mail são interpretadas depende muito do tipo de rede que utiliza. Vamos nos concentrar em como TCP / IP e redes UUCP interpretar os endereços de e-mail.

RFC-822

sites da Internet aderir à norma RFC-822, que exige a notação de user@host.domain familiar, por
host.domain que é o nome do host de domínio totalmente qualificado. O caractere que separa os dois é chamado corretamente um "comercial em" assinar, mas ajuda se você ler como "no". Esta notação não especificar uma rota para o destino host. Roteamento da mensagem de correio é deixada aos mecanismos iremos descrever brevemente.

Você vai ver um monte de RFC-822 se você executar um site conectado à Internet. Seu uso não se estende apenas ao correio, mas também
repercutiu em outros serviços, como notícias. Discutimos como RFC-822 é usada para a notícia no Capítulo 20, *Net-notícias*.

Obsoleto formatos de email

No ambiente UUCP original, a forma mais encontrada foi a caminho! Usuário host!, Para o qual caminho descrito uma seqüência
dos Exércitos a mensagem teve de percorrer antes de atingir o host de destino. Esta construção é chamada de *Bang caminho* notação, pois um ponto de exclamação é coloquialmente chamado de "bang". Hoje, muitas redes baseadas UUCP adotaram RFC-822 e compreender os endereços baseados em domínio.

Outras redes ainda dispõem de meios diferentes de endereçamento. DECnet redes baseadas, por exemplo, usar dois dois pontos como
um separador de endereços, gerando um endereço de host: usuário.[109] O padrão X.400 utiliza um esquema completamente diferente,
descrevendo um receptor por um conjunto de pares atributo-valor, como país e da organização.

Por último, em FidoNet, cada usuário é identificado por um código como *2:320 / 204.9*, Constituído de quatro números que denotam zona
(2 é para a Europa), líquido (320 sendo Paris e Banlieue), nó (o centro local), e do ponto (PC do usuário individual). Fidonet endereços podem ser mapeados para RFC-822, acima, por exemplo, seria escrito como Tho-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

mas.Quinot @ p9.f204.n320.z2.fidonet.org. Agora não podemos dizer os nomes de domínio foram fáceis de lembrar?

108 Isso ocorre porque o espaço em disco é geralmente distribuídas em blocos de 1.024 bytes. Assim, mesmo uma mensagem de uma dúzia de bytes poucos vai comer um kilobyte completo.

109 Ao tentar chegar a um endereço DECnet de um RFC-822 ambiente, você pode usar o "host:" user @ revezamento, no qual o relé é o nome de um conhecido revezamento DECnet Internet.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Misturando diferentes formatos de email

É inevitável que, quando você reúne uma série de sistemas diferentes e um número de pessoas inteligentes, eles irá buscar meios para interligar os diferentes sistemas que eles são capazes de internetworking. Por conseguinte, não um grande número de gateways de correio diferentes que são capazes de ligar dois sistemas de email diferentes ao mesmo tempo, para que e-mail
pode ser transmitida de um para outro. Dirigindo-se a questão crítica quando liga dois sistemas. Nós não olhar para os gateways se em qualquer detalhe, mas vamos dar uma olhada em algumas das complicações de endereçamento que podem surgir quando gateways desse tipo são usadas.

Considere a mistura do estilo UUCP notação de caminho-bang e RFC-822. Estes dois tipos de abordagem não se misturam muito
também. Suponha que há um endereço de domainA! DomainB user @. Não está claro se o sinal @ prevale-dência ao longo do caminho, ou vice-versa: que temos que enviar a mensagem para domainB, que envia para domainA usuário! ou deverá ser enviado para domainA, que encaminha para o usuário domainB @?

Os endereços que misturam tipos diferentes de operadores de endereço são chamados *endereços híbrido*. O tipo mais comum, que acabamos de ilustrados, geralmente é resolvido dando a primazia sinal @ ao longo do caminho. Em se-mainA! usuário @ domainB, isto significa enviar a mensagem para domainB primeiro.

No entanto, existe uma maneira de especificar as rotas na RFC-822 conformant maneiras:
<@ DomainA, domainB @ user @ domainC> denota o endereço do usuário no domainC, onde domainC deve ser alcançado através domainA e domainB (nessa ordem). Esse tipo de endereço é freqüentemente chamado de *a rota de origem* endereço. Não é uma boa idéia de contar com esse comportamento, como a revisão do RFC descreve o roteamento de correio reco-
Recomendamos que o roteamento de origem em um endereço de e-mail deve ser ignorado e em vez disso uma tentativa deve ser feita para entregar directamente
para o destino remoto.

Depois, há o operador de endereço%:% user domainB domainA @ é enviada para domainA, que expande o mais à direita (neste caso, a única) por cento, para assinar um sinal @. O endereço é agora *user @ domainB*E mailer a felizmente encaminha sua mensagem para domainB, que entrega-lo para o usuário. Esse tipo de endereço algumas vezes é chamado
como "Ye Olde ARPAnet Kludge", e seu uso é desencorajado.

Há algumas implicações para a utilização desses diferentes tipos de endereçamento que será descrito todo o nas seções seguintes. Em um ambiente RFC-822, você deve evitar usar qualquer coisa diferente de endereços absolutos, como user@host.domain.

Como o Correio de roteamento funciona?

O processo de dirigir uma mensagem ao host do destinatário é chamado *roteamento*. Além de encontrar um caminho do enviar para o site de destino, que envolve a verificação de erros e pode envolver velocidade e otimização de custos.

Há uma grande diferença entre a maneira como um site UUCP manipula roteamento ea maneira como um site na Internet faz. Na Internet, o trabalho principal de direcionar os dados para o host destinatário (uma vez que é conhecida por seu endereço IP) é feito pelo IP camada de rede, enquanto na zona UUCP, o percurso tem de ser fornecida pelo usuário ou gerado pelo e-mail
agente de transferência.

Mail Roteamento na Internet

Na Internet, a configuração do host de destino determina se as mensagens específicas de roteamento é realizado.
O padrão é para entregar a mensagem para o destino de primeiramente determinar o acolhimento da mensagem deve ser enviada para em seguida, entregá-la diretamente para o host. A maioria dos sites da Internet quer direcionar todas as mensagens de entrada para um proveito altamente
servidor de correio capaz que seja capaz de lidar com todo esse tráfego e tê-lo distribuir o correio localmente. Para anunciar esta serviço, o site publica um chamado registro MX para seu domínio local em seu banco de dados DNS. MX representa *Mail Permutador* e, basicamente, afirma que a máquina servidora está disposta a atuar como um encaminhador de email para todos os endereços de e-mail
o domínio. Os registros MX também pode ser usado para lidar com o tráfego de hosts que não estão conectados à Internet-los mesmos, como redes ou hosts UUCP FidoNet que deve ter seu e-mail passado por um gateway.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Os registros MX é sempre atribuído um *preferência*. Este é um número inteiro positivo. Se existirem vários trocadores mail para

um

hospedeiro, o agente de transporte de correio irá tentar transferir a mensagem para o trocador com o menor valor de preferência, e somente se isso não vai tentar um host com um valor superior. Se o host local é próprio de um trocador de correio para o desti- Endereço nação, é permitido apenas para encaminhar mensagens para hosts MX com menor preferência diferente da sua, este é um

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

maneira segura de evitar loops e-mail. Se não houver nenhum registro MX para um domínio, ou nenhuma registros MX esquerda que são adequados,
o agente de transporte de correio tem permissão para ver se o domínio tem um endereço IP associado a ele e entregas tentativa-
ery diretamente para o host.

Suponha que uma organização, digamos Foobar, Inc., quer todos os seus correio tratado pela sua máquina *mailhub*. Em seguida,

será
tem registros MX como esta no banco de dados DNS:

```
green.foobar.com.        EM    MX      5     mailhub.foobar.com.
```

Este anuncia *mailhub.foobar.com* como um trocador de e-mail para *green.foobar.com* com uma preferência de 5. Um host que pretende entregar uma mensagem ao DNS verifica joe@green.foobar.com e encontra o registro MX apontando para *mailhub*. Se não houver MX com uma preferência inferior a 5, a mensagem é entregue *mailhub*, Que então despacha-lo para *verde*.

Esta é uma descrição muito simples de como funcionam os registros MX. Para mais informações sobre o roteamento de correio

na inter-
NET, consulte a RFC-821, RFC-974 e RFC-1123.

Mail roteamento no Mundo UUCP

Mail roteamento em redes UUCP é muito mais complicado do que na internet porque o software de transporte
não realizar qualquer encaminhamento próprio. Em outros tempos, todo o correio tinha que ser abordada através de caminhos bang. caminhos Bang
especificada uma lista de hosts através do qual a transmitir a mensagem, separados por pontos de exclamação e seguido por o nome do usuário. Para enviar uma carta a um usuário chamado Janet em uma máquina chamada *moria*, Você poderia usar o caminho
eek! nadar! moria! janet. Este seria enviar o e-mail de seu anfitrião *eek*, A partir daí a *nadar*E, finalmente, *moria*.

A desvantagem óbvia dessa técnica é que ela exige que você se lembra muito mais sobre a topologia da rede,
ligações rápidas, etc de roteamento da Internet requer. Muito pior do que isso, mudanças na topologia da rede - ligações como sendo excluído ou hosts a ser removido - pode causar mensagens de falhar simplesmente porque você não está ciente da mudar. E, finalmente, no caso de você ir para um lugar diferente, você provavelmente terá de atualizar todas as rotas.

Uma coisa, porém, que fez o uso da fonte de encaminhamento necessário foi a presença de nomes de máquinas ambígua.
Por exemplo, suponha que há dois sites nomeados *moria*, Um em os EUA e um na França. Qual site faz
moria! janet referem-se agora? Isto pode ficar claro ao especificar qual o caminho para chegar *moria* completamente.

O primeiro passo para hostnames disambiguating foi o fundador do Projeto de Mapeamento UUCP. Ele está localizado na Rut-
gers Universidade e registra todos os hostnames oficial UUCP, juntamente com informações sobre seus vizinhos UUCP e sua localização geográfica, fazendo com que não se hostname é utilizado duas vezes. As informações recolhidas pelo mapeamento
Projeto é divulgado como *Usenet Maps*, Que são distribuídos regularmente através da Usenet. A entrada do sistema típico em um mapa (depois de remover os comentários) fica assim:[110]

```
moria
        bert (DIÁRIO / 2),
        nadar (semanal)
```

Essa entrada, diz *moria* tem um link para *bert*, Que ele chama duas vezes por dia, e *nadar*, Que ele chama semanais. Nós voltar ao formato de arquivo de mapa com mais detalhes posteriormente.

Usando as informações fornecidas conectividade nos mapas, é possível gerar automaticamente os caminhos completos de seu anfitrião para qualquer site de destino. Esta informação é normalmente armazenado no *caminhos* arquivo, também chamado de *pathalias*
banco de dados. Suponha que o estado de mapas que você pode alcançar *bert* através *Ernie*; Uma entrada para pathalias *moria*
Geração
No trecho de mapa anterior pode então ser algo parecido com isto:

```
moria           Ernie! bert! moria!% s
```

Se você agora dar um endereço de destino janet@moria.uucp, o MTA irá escolher o percurso acima e enviar a mensagem para *Ernie* envelope com um endereço de bert! moria! janet.

A construção de uma *caminhos* arquivo a partir de mapas completos da Usenet não é uma tarefa muito boa, no entanto. As

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

informações fornecidas na

eles é geralmente bastante distorcida e, ocasionalmente, fora da data. Portanto, apenas um número de hospedeiros importantes de utilização da

mapas do mundo completa UUCP para construir a sua *caminhos* arquivos. A maioria dos sites mantêm informações de roteamento apenas para sites

seu bairro e enviar e-mail para sites que não encontram em suas bases de dados para um host inteligente, com mais com-

110 Mapas para sites registrados com o Projeto de Mapeamento UUCP são distribuídos através do comp.mail.maps newsgroup; outras organizações pode publicar mapas separados para suas redes.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

completo de informações de roteamento. Esse sistema é chamado *host-roteamento inteligente*. Os hosts que tem apenas um link de email UUCP
(Os chamados *sites folha*) Não fazem nenhum encaminhamento do seu próprio, pois eles dependem inteiramente do seu host inteligente.

Misturando UUCP e RFC-822

A melhor cura para os problemas de roteamento de mensagens em redes UUCP medida é a adoção do nome de domínio sistema em redes UUCP. Claro, você não pode um servidor de consulta de nome sobre o UUCP. UUCP No entanto, muitos sites formaram pequenos domínios que coordenam suas roteamento internamente. Nos mapas, esses domínios anunciar hospeda um ou dois como seus gateways de email, para que não tem de ser uma entrada de mapa para cada máquina no domínio. Os gateways lidar com todos os emails que flui para dentro e fora do domínio. O esquema de roteamento dentro do domínio é completamente invisível para o mundo exterior.

Isso funciona muito bem com o host inteligente esquema de roteamento. Global encaminhamento informação é mantida pelo portão
únicas maneiras; hosts menores dentro de um domínio se dá bem com apenas um pequeno manuscrito *caminhos* arquivo que lista as rotas
dentro de seu domínio eo caminho para o centro de correio. Até mesmo os gateways de correio não precisam de encaminhamento de informações para
cada host UUCP única no mundo mais. Além das informações completas de roteamento para o domínio que servir, eles só precisam ter rotas para domínios inteiros em suas bases de dados agora. Por exemplo, esta entrada pathalias irá encaminhar todos os e-mail para sites no *sub.org* domínio *smurf*:

```
. Sub.org       nadar! smurf!% s
```

Correspondência dirigida à claire@jones.sub.org será enviado para *nadar* envelope com um endereço de smurf! Jones! Claire.

A organização hierárquica do namespace do domínio permite que os servidores de correio para misturar as rotas mais específicas com menos
mais específicas. Por exemplo, um sistema em França pode ter rotas específicas para os subdomínios *fr*, Rota, mas qualquer e-mail
para os anfitriões no *nos* domínio em direção a algum sistema em os EUA Desta forma, baseado no domínio de roteamento (como esta técnica
é chamado) reduz o tamanho das bases de dados de roteamento, bem como as despesas gerais administrativas necessárias.

O principal benefício da utilização de nomes de domínio em um ambiente de UUCP, porém, é que a conformidade com RFC-822
permite fácil gatewaying UUCP entre redes e na Internet. Muitos domínios UUCP hoje em dia têm uma ligação
com um gateway de internet que atua como o host inteligente. O envio de mensagens através da Internet é mais rápido, e encaminhamento
informação é muito mais confiável porque os anfitriões Internet pode usar DNS em vez dos Mapas da Usenet.

A fim de ser acessível a partir da Internet, os domínios UUCP baseado geralmente têm seu gateway Internet anunciar
um registro MX para eles (os registros MX foram descritas anteriormente na seção "Encaminhamento de correio na Internet").
Por exemplo, suponha que *moria* pertence à *orcnet.org* domínio. *gcc2.groucho.edu* age como seu gateway de Internet.
moria Por conseguinte, o uso *gcc2* como seu host inteligente, para que todo o correio para domínios estrangeiros é emitido através do
Internet. Por outro lado, *gcc2* anunciaria um registro MX para **. Orcnet.org* e entregar todos os e-mails recebidos
para *orcnet* sites para *moria*. O asterisco na **. Orcnet.org* É um curinga que corresponde a todos os hosts nesse domínio que não têm qualquer outro registro que lhes estão associados. Isto deve ser normalmente o caso para domínios UUCP-somente.

O único problema é que os programas de transporte UUCP não pode lidar com nomes de domínio totalmente qualificado.
A maioria das suites UUCP foram projetadas para lidar com nomes de sites de até oito caracteres, alguns menos ainda, e utilizando
caracteres alfanuméricos, tais como pontos é completamente fora de questão para a maioria.

Portanto, precisamos de mapeamento entre RFC-822 nomes e nomes de máquinas UUCP. Esse mapeamento é completamente im-
plementação-dependente. Uma maneira comum de mapeamento de nomes FQDNs UUCP é usar o arquivo pathalias:

```
moria.orcnet.org  Ernie! bert! moria!% s
```

Isso produz um bang UUCP puro estilo de um endereço que especifica um nome de domínio totalmente qualificado.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Alguns utentes fornecer um arquivo especial para isso; `sendmail`, Por exemplo, usa o *uucpxtable*.

A transformação inversa (coloquialmente chamado *domainizing*) Às vezes é necessária quando o envio de um e-mail UUCP rede à Internet. Enquanto o remetente do email usa o nome de domínio totalmente qualificado no destino endereço, esse problema pode ser evitado por não retirar o nome de domínio do endereço de envelope, quando for-defender a mensagem para o host inteligente. No entanto, ainda existem alguns sites UUCP que não fazem parte de qualquer domínio.
Eles são geralmente domainized anexando o pseudo-domínio *uucp*.

O banco de dados pathalias fornece as principais informações de roteamento em redes baseadas UUCP. Uma entrada típica se parece
como este (nome do site eo caminho são separadas por abas):

```
moria.orcnet.org  Ernie! bert! moria!% s
moria             Ernie! bert! moria!% s
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Isso faz com que qualquer mensagem de *moria* ser entregue via *Ernie* e *bert*. Ambos *moria*É totalmente qualificado nome e sua UUCP nome tem que ser dada se o envelope não tem uma maneira separada para mapear entre esses espaços.

Se você deseja direcionar todas as mensagens para hosts dentro de um domínio para a sua retransmissão de email, você também pode especificar um caminho no pathalias banco de dados, dando o nome de domínio precedido por um ponto como o destino. Por exemplo, se todos os hosts *sub.org* pode ser alcançado através *nadar! smurf*, A entrada pathalias pode ter este aspecto:

```
. Sub.org       nadar! smurf!% s
```

Escrevendo um arquivo pathalias é aceitável somente quando você estiver executando um site que não tem que fazer muito roteamento. Se você tem que fazer encaminhamento para um grande número de hospedeiros, a melhor maneira é usar o `pathalias` comando para criar o arquivo a partir de arquivos do mapa. Os mapas podem ser mantidos com muito mais facilidade, porque você pode simplesmente adicionar ou remover um sistema de edição de entrada do sistema de mapas e recriar o arquivo de mapa. Embora os mapas publicados pelo Uso net Mapping Project não são utilizados para roteamento muito mais, redes menores UUCP pode fornecer roteamento informações em seu próprio conjunto de mapas.

Um arquivo de mapa consiste principalmente de uma lista de sites que cada sistema de enquetes ou é sondado por. O nome do sistema se inicia no primeira coluna e é seguido por uma lista separada por vírgulas de links. A lista pode ser continuada em novas linhas se o próxima linha começa com um guia. Cada link contém o nome do site seguido por um custo entre parênteses. A custo é uma expressão aritmética composta de números e expressões simbólicas, como diário ou semanal. Linhas começando com um cardinal são ignorados.

Como exemplo, considere *moria*, Que as pesquisas *swim.twobirds.com* duas vezes ao dia e *bert.sesame.com* uma vez por semana.
O link para *bert* usa um modem lento 2.400 bps. *moria* a publicar a entrada os seguintes mapas:

```
moria.orcnet.org
        bert.sesame.com (DIÁRIO / 2),
        swim.twobirds.com (semanal + BAIXO)
moria.orcnet.org = moria
```

A última linha faz *moria* conhecido pelo seu nome UUCP, também. Note-se que o seu custo deve ser especificado como *DIÁRIO / 2* porque chamar duas vezes por dia, na verdade reduz pela metade o custo para este link.

Usando as informações dos arquivos de mapa tal, `pathalias` é capaz de calcular as melhores rotas para qualquer destino site listado nos caminhos de arquivo e produzir um banco de dados pathalias deste que pode então ser utilizada para o encaminhamento destes sites.

`pathalias` fornece um par de outras características como esconder-site (ou seja, fazer sites acessíveis apenas através de um gateway). Veja o `pathalias` página de manual para mais detalhes e uma lista completa dos custos de ligação.

Comentários no arquivo de mapa em geral contêm informações adicionais sobre os locais descritos no mesmo. Existe uma rígida formato no qual deseja especificar estas informações para que elas possam ser recuperadas a partir dos mapas. Por exemplo, um programa chamada `uuwho` usa um banco de dados criado a partir de arquivos de mapa para mostrar essa informação de uma maneira bem formatada.
Quando você registrar seu site com uma organização que distribui os arquivos de mapas para os seus membros, geralmente você tem que preencher essa entrada um mapa. Abaixo está uma entrada de mapa de exemplo (na verdade, é o único site de Olaf):

```
# N             # L
# S             # U
# O             # W
C #             #
# E
# P
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
monad.swb.de,   0,99
                privada
mônada,         Olaf Kirch
monad.swb.sub.  okir@monad.swb.de
org             Kattreinstr. 38, D-64295 Darmstadt, FRG
                49 52 03 N / 08 38 40 E
AT              brewhq
configuração:   okir@monad.swb.de (Olaf Kirch); dom 25 jul 1993 16:59:32 MET DST
486DX50; Linux
      mónada    brewhq (DIÁRIO / 2)
      Domínios #
      mônada = monad.swb.de
      mônada = monad.swb.sub.org
```

O espaço em branco após os dois primeiros caracteres é um guia. O significado da maioria dos campos é bastante óbvio, você vai receber uma descrição detalhada a partir de qualquer domínio que você registrar. A *L* campo é o mais divertido para encontrar

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Saída: ele dá a sua posição geográfica em latitude / longitude e é usada para desenhar os mapas que mostram PostScript todos os sites de cada país, bem como todo o mundo.[111]

Configurando elm

`olmo` está para "correio electrónico" e é uma das ferramentas mais razoavelmente chamado Unix. Ele fornece uma tela cheia interface com um recurso boa ajuda. Nós não vamos discutir como usar `olmo` aqui, mas apenas insistir em sua configuração opções.

Teoricamente, você pode executar `olmo` desconfigurado, e tudo funciona bem - se você tiver sorte. Mas há alguns opções que devem ser definidas, embora sejam necessários apenas em algumas ocasiões.

Quando ela começa, `olmo` lê um conjunto de variáveis de configuração do *elm.rc* arquivo em */ Elm / etc*. Em seguida, ele tenta ler o arquivo *.elm / elmrc* em seu diretório home. Você não costumo escrever esse arquivo. Ele é criado quando você escolha "Salvar opções novas" a partir de `olmo`'S menu de opções.

O conjunto de opções para o privado *elmrc* arquivo também está disponível no mercado global *elm.rc* arquivo. A maioria das configurações em seu pri- vate *elmrc* ficheiro de substituir os do arquivo global.

Opções globais elm

No global *elm.rc* arquivo, você deve definir as opções que dizem respeito ao nome do seu anfitrião. Por exemplo, no Virtual Cervejaria, o arquivo para *vlager* contém o seguinte:

```
#
# O nome do host local
vlager hostname =
#
# Nome do domínio
= hostdomain. vbrew.com
#
# Nome de domínio totalmente qualificado
vlager.vbrew.com hostfullname =
```

Essas opções definem `olmo`"Ideia s do nome do host local. Embora esta informação raramente é usado, você deve definir o opções. Note que estas opções particular só produzirá efeitos quando dá-los no arquivo de configuração global; quando foi encontrado em sua privada *elmrc*, Eles serão ignorados.

Conjuntos de caracteres nacionais

Um conjunto de normas e RFC foram desenvolvidos para alterar a norma RFC-822 para apoiar diversos tipos de mensagens, tais como texto, dados binários, arquivos PostScript, etc Esses padrões são comumente referido como MIME, ou Multipurpose Internet Mail Extensions. Entre outras coisas, MIME também permite que o destinatário saiba se um conjunto de caracteres que não sejam ASCII padrão tem sido usado quando se escreve a mensagem, por exemplo, usando o francês acentos ou umlauts Alemães. `olmo` suporta esses personagens até certo ponto.

O conjunto de caracteres usado pelo Linux internamente para representar caracteres é normalmente referida como ISO-8859-1, que é o nome do padrão, ele obedece. É também conhecido como Latin-1. Qualquer mensagem com caracteres a partir deste conjunto de caracteres deverá ter a seguinte linha em seu cabeçalho:

```
Content-Type: text / plain; charset = iso-8859-1
```

~~O sistema de recebimento deve reco~~nhecer este campo e tomar as medidas adequadas ao exibir a mensagem. O padrão para *text / plain* mensagens é um *charset* valor de *us-ascii*.

Para ser capaz de exibir mensagens com conjuntos de caracteres que não sejam ASCII, `olmo` deve saber como imprimir estas

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

carac-
tros. Por padrão, quando `olmo` recebe uma mensagem com um *charset* outro campo de *us-ascii* (Ou um outro tipo de conteúdo

111 Eles são postadas regularmente no news.lists.ps-maps. Cuidado. Eles são enormes.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

que *text / plain*, Para que o assunto), ele tenta exibir a mensagem usando um comando chamado `metamail`. Mensagens que requerem `metamail` a serem exibidos são mostrados com um `M` na coluna de primeira na tela de síntese.

Uma vez definido o caráter Linux nativo é ISO-8859-1, chamando `metamail` não é necessário para exibir mensagens usando esse conjunto de caracteres. Se `olmo` é dito que a exibição compreende ISO-8859-1, ele não vai usar `metamail`, Mas exibir a mensagem diretamente em seu lugar. Isso pode ser ativada por definição a seguinte opção no mercado global *elm.rc*:

```
displaycharset = iso-8859-1
```

Observe que você deve definir essa opção, mesmo quando você nunca vai enviar ou receber mensagens que realmente conter caracteres que não sejam ASCII. Isto é porque as pessoas que enviam essas mensagens normalmente configurar seus envelope para colocar o bom `Tipo de conteúdo:` de campo no cabeçalho de correio por padrão, ou não estão enviando mensagens somente ASCII.

No entanto, definir esta opção em *elm.rc* não é suficiente. Ao exibir a mensagem com sua base de pager, `olmo` chama uma função de biblioteca para cada personagem para determinar se é impressão. Por padrão, essa função só reconhecer caracteres ASCII imprimíveis e mostrar como todos os outros personagens `^?`. Você pode superar esta função definindo a variável de ambiente *LC_CTYPE* para *ISO-8859-1*, Que narra a biblioteca para aceitar Latina carac-1-tros como impressão. Suporte para este e outros recursos estão disponíveis desde a versão 4.5.8 do Linux stan-biblioteca padrão.

Ao enviar mensagens que contêm caracteres especiais da ISO-8859-1, você deve certificar-se de definir mais dois variáveis no *elm.rc* arquivo:

```
charset = iso-8859-1
textencoding = 8bit
```

Isso faz com que `olmo` relatório o conjunto de caracteres ISO-8859-1 no cabeçalho da mensagem e enviá-lo como um valor de 8 bits (o de-
culpa é tirar todos os caracteres de 7 bits).

Claro, todo o caráter definir as opções que temos discutido aqui também pode ser definida no privado *elmrc* arquivo em vez do um global para que os usuários individuais podem ter suas próprias configurações padrão, se o global não lhes agrada.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 18 - Sendmail

Introdução ao sendmail

Tem sido dito que você não é um *real* Administradores de sistemas Unix até que você tenha editado um *sendmail.cf* arquivo.

Também foi
disse que você é louco se você já tentou fazer isso duas vezes.

`sendmail` é um programa de correio incrivelmente poderoso. Ele também é incrivelmente difícil de aprender e compreender. Qualquer
programa cujo definitiva de referência (`sendmail`, Por Bryan Costales e Eric Allman, publicado pela O'Reilly) é 1.050 páginas assusta mais as pessoas. Informações sobre o `sendmail` referência está contida na bibliografia, fia no final deste livro.

Felizmente, as novas versões do sendmail são diferentes. Você não precisa editar diretamente o enigmático *sendmail.cf* ficheiro, a nova versão fornece um utilitário de configuração que irá criar o *sendmail.cf* arquivo para você, baseado em muito simples arquivos de macro. Você não precisa entender a sintaxe complexa do *sendmail.cf* arquivo, os arquivos de macro não exigem que você. Em vez disso, você precisa apenas os itens da lista, como o nome das características que você deseja incluir em seu
configuração, e especificar alguns dos parâmetros que determinam como o recurso funciona. A tradicional do Unix utilitário chamado `m4` em seguida, toma os dados de configuração macro e mistura-lo com os dados que ele lê arquivos de modelo
contendo o real *sendmail.cf* sintaxe, para produzir o seu *sendmail.cf* arquivo.

Neste capítulo, vamos introduzir `sendmail` e descrever como instalar, configurar e testar, usando o Virtual Cervejaria como um exemplo. Se as informações apresentadas aqui ajuda a tornar a tarefa de configurar `sendmail` menos difícil para você, esperamos que você vai ganhar a confiança necessária para lidar com configurações mais complexas no seu próprio país.

Instalando o sendmail

A `sendmail` agente de transporte de correio está incluído no formulário de pré-na maioria das distribuições Linux. Instalação

em
Neste caso é relativamente simples. Apesar disso, existem algumas boas razões para se instalar `sendmail` de fonte, especialmente se você estiver consciente de segurança. A `sendmail` programa é muito complexo e tem uma reputação ao longo dos anos por conter bugs que permitem violações de segurança. Um dos exemplos mais conhecidos é o RTM Internet worm que exploravam um problema de estouro de buffer nas versões anteriores do `sendmail`. Nós tocamos nesse assunto
brevemente no capítulo 9, *Firewall TCP / IP*. A maioria dos exploits de segurança envolvendo o buffer overflows confiar em todas as cópias do
`sendmail` em máquinas diferentes são idênticas, como as aventuras se baseiam em dados sejam armazenados em locais específicos.
Isso, é claro, é precisamente o que acontece com `sendmail` instalado a partir de distribuições Linux. Compilando `sendmail` do fonte pode ajudar a reduzir esse risco. Versões modernas de `sendmail` são menos vulneráveis porque eles estão sob escrutínio muito parecida como a segurança se tornou uma preocupação mais ampla toda a comunidade da Internet.

A `sendmail` código fonte está disponível via FTP anônimo ftp.sendmail.org.

A compilação é muito simples o bceause `sendmail` pacote fonte diretamente suporta Linux. As etapas envolvidas na compilação `sendmail` são:

```
# Cd / usr / local / src
# Tar xvfz sendmail.8.9.3.tar.gz
# Cd src
#. / Build
```

Você precisa `root` permissões para concluir a instalação dos arquivos binários resultantes usando:

```
# Cd obj.Linux.2.0.36.i586
# Make install
```

Você já instalou o `sendmail` binários na */ Usr / sbin* diretório. Vários

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`e-mail` binário será instalado na */ Usr / bin /* diretório. Falaremos sobre essas relações quando discutimos comum tarefas em execução `sendmail`.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Visão geral dos arquivos de configuração

Tradicionalmente, os `sendmail` foi criada através de um arquivo de configuração do sistema (geralmente chamado */ Etc / mail / sendmail.cf*, ou de distribuições mais antigas, */ Etc / sendmail.cf*, Ou mesmo */ Usr / lib / sendmail.cf*) Que não é nada perto de todas as línguas você já viu antes. Editando o *sendmail.cf* arquivo para fornecer o comportamento personalizado pode ser uma experiência humilhante.

Hoje `sendmail` faz todas as opções de configuração macro conduzido com um fácil de entender a sintaxe. A macro método gera configurações para cobrir a maioria das instalações, mas você sempre tem a opção de ajustar o resultant *sendmail.cf* manualmente para trabalhar em um ambiente mais complexo.

O sendmail.cf e arquivos sendmail.mc

A `m4` programa de processador de macro gera o *sendmail.df* arquivo quando ele processa o arquivo de configuração do macro fornecidas pelo administrador do sistema local. Ao longo do restante deste capítulo vamos referir a esta configuração arquivo de configuração como a *sendmail.mc* arquivo.

O processo de configuração é basicamente uma questão de criar uma adequada *sendmail.mc* arquivo que inclui macros que descrever a sua configuração desejada. As macros são expressões que a `m4` processador de macro compreende e expande para o complexo *sendmail.cf* sintaxe. As expressões macro são compostas do nome da macro (o texto em letras maiúsculas no início), que pode ser comparado a uma função em uma linguagem de programação, e alguns parâmetros (O texto entre parênteses) que são utilizados na expansão. Os parâmetros podem ser passados literalmente para o *Enviar-mail.cf* saída ou pode ser usada para reger a forma como ocorre o processamento de macro.

A*sendmail.mc* arquivo para uma configuração mínima (UUCP ou SMTP mail com todos os não-local a ser retransmitida para uma di-
de forma incorreta host inteligente) pode ser tão curto quanto 10 ou 15 linhas, excluindo comentários.

Dois arquivos de exemplo sendmail.mc

Se você é um administator de um número de servidores de email diferente, você não pode querer o nome do seu arquivo de configuração
sendmail.mc. Em vez disso, é prática comum para nomeá-la depois do hospedeiro - *vstout.m4* em nosso caso. O nome não realmente importa, desde que a saída é chamado *sendmail.cf*. Fornecer um nome exclusivo para o arquivo de configuração para cada host permite-lhe manter todos os arquivos de configuração no mesmo diretório e é apenas uma convenção administrativo-IENCE. Vejamos dois arquivos de configuração de exemplo macro assim que nós sabemos para onde estamos indo.

A maioria dos `sendmail` configurações de SMTP usam hoje somente. É muito simples de configurar `sendmail` para SMTP. Exemplo de 18,1 expectos um servidor de nome DNS para estar disponível para resolver hosts e tentará aceitar e entregar e-mail para todos os hosts utilizando apenas SMTP.

Exemplo 18.1: Exemplo de arquivo de configuração vstout.smtp.m4

```
divert (-1)
#
# Exemplo de arquivo de configuração para vstout - smtp só
#
Desvio (0)
VERSIONID (`@(#) sendmail.mc    8,7 (Linux) 3/5/96)
OSTYPE (linux)
#
# Inclui suporte para os protocolos de transporte local e SMTP de correio.
Mailer («local»)
MAILER (smtp `')
#
FEATURE (RBL)
FEATURE (access_db)
# Fim
```

A *sendmail.mc* arquivo para o *vstout* na Cervejaria virtual é mostrado na Exemplo 18.2, "vstout SMTP.m4" para conversar com todos

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

os
hosts na LAN da cervejaria, e você verá a semelhança com a configuração genérica SMTP apenas
apresentados. Além disso, o *vstout* configuração envia todas as mensagens para outros destinos a *moria*, A sua retransmissão Internet
acolhimento, através de UUCP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Exemplo 18.2: Exemplo de arquivo de configuração vstout.uucpsmtp.m4

```
divert (-1)
#
# Arquivo de configuração de exemplo para vstout
#
Desvio (0)
VERSIONID (`@(#) sendmail.mc    8,7 (Linux) 3/5/96)
OSTYPE (linux)
dnl
moria # é o nosso host inteligente, usando o "uucp novo" transporte.
define (`SMART_HOST ',` uucp-novo: moria ")
dnl
# Suporte a smtp, local e protocolos de transporte de correio uucp.
Mailer («local»)
MAILER (smtp `')
MAILER (`uucp ')
LOCAL_NET_CONFIG
# Esta regra garante que toda a correspondência é entregue local usando o
# Transporte SMTP, tudo o resto vai passar pelo host inteligente.
R $ * <* @ $ $. M. > $ *  smtp $ # $ @ $ 2 $. m. $:. $ 1 <@ $ 2 $ m. > $
3
dnl
#
FEATURE (RBL)
FEATURE (access_db)
# Fim
```

Se você comparar e contrastar as duas configurações, você pode ser capaz de descobrir o que cada uma das configura-
parâmetros ção faz. Vamos explicar tudo em detalhes.

Normalmente usado Parâmetros sendmail.mc

Alguns dos itens da *sendmail.mc* arquivo é necessário o tempo todo, enquanto outros podem ser ignorados se você pode ir longe com padrões. A seqüência geral das definições do *sendmail.mc* é o seguinte:

1. *VERSIONID*
2. *OSTYPE*
3. *DOMAIN*
4. *RECURSO*
5. Local definições de macro
6. *MAILER*
7. *LOCAL_ * *rulesets

Falaremos sobre cada um destes aspectos nas seções seguintes e referem-se aos nossos exemplos Exemplo de 18,1 umd Exemplo 18.2,quando apropriado, para explicá-los.

Comentários

As linhas do *sendmail.mc* arquivos que começam com a # caracteres não são analisados pelo `m4`E, por padrão será a saída diretamente na *sendmail.cf* arquivo. Isso é útil se você quiser comentar sobre o que a configuração está fazendo em ambos os arquivos de entrada e saída.

Para permitir que os comentários no seu *sendmail.mc* que são *não* colocado no *sendmail.cf*, Você pode usar o `m4` *desviar* e *dnl* tokens. *divert (-1)* fará com que toda a saída para acabar. *Desvio (0)* fará com que a saída para ser restaurado para o padrão. Qualquer
saída gerada por linhas entre estes serão descartados. No nosso exemplo, usamos este mecanismo para fornecer um comentário que só aparece na *sendmail.mc* arquivo. Para alcançar o mesmo resultado para uma única linha, você pode usar o *dnl* símbolo que significa, literalmente, "a partir do início da próxima linha, apagar todos os caracteres até e incluindo a o fim da linha. "Nós usamos isso em nosso exemplo, também.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Trata-se de norma `m4` características, e você pode obter mais informações sobre eles a partir de sua página de manual.

VERSIONID e OSTYPE

```
VERSIONID (`@(#) sendmail.mc  8,9 (Linux) 01/10/98)
```

A `VERSIONID` macro é opcional, mas é útil para gravar a versão da configuração do sendmail no *sendmail.cf* arquivo. Então muitas vezes você vai encontrá-lo, e nós recomendamos ele. Em qualquer caso, não se esqueça de incluir:

```
OSTYPE (linux)
```

Esta é provavelmente a definição mais importante. A `OSTYPE` macro faz com que um arquivo de definições a serem incluídos que são bons valores por omissão para o seu sistema operacional. A maioria das definições em um `OSTYPE` arquivo da macro definir o caminho
nomes de vários arquivos de configuração, os caminhos mailer programa e argumentos, bem como a localização dos diretórios envio
e-mail usa para armazenar mensagens. O padrão sendmail liberar o código fonte inclui um ficheiro deste tipo para Linux, que seria incluído pelo exemplo anterior. Algumas distribuições de Linux, nomeadamente a distribuição Debian, incluir
sua própria definição de arquivo que é totalmente compatível com Linux, FHS. Quando a sua distribuição faz isso, você deve provavelmente usará sua definição ao invés do padrão do Linux.

A *OSTYPE* definição deve ser uma das primeiras definições para aparecer na sua *sendmail.mc* arquivo, como muitos outros definições dependem dela.

DOMAIN

A *DOMAIN* macro é útil quando você deseja configurar um grande número de máquinas na mesma rede em um forma padrão. É que você está configurando um pequeno número de hosts, ele provavelmente não vale a pena incomodar-se com. Você normalmente
configurar itens, como o nome de hosts e encaminhar o correio ou hubs que todos os hosts em sua rede vai usar.

A instalação padrão contém um diretório de `m4` macro modelos usados para conduzir o processo de configuração. Este diretório é geralmente chamado */ Usr / share / sendmail.cf* ou algo semelhante. Aqui você encontrará um subdiretório chamada *domínio* que contém configuração de domínio modelos específicos. Para fazer uso do *DOMAIN* macro, você deve criar seu próprio arquivo macro que contém as definições padrão que você precisa para o seu site, e escrevê-lo em o *domínio* subdiretório. Você normalmente incluem apenas as definições de macro que eram exclusivas de seu domínio aqui, tais como definições de host inteligente ou hosts de revezamento, mas não estão limitados a estes.

A `sendmail` distribuição do código fonte vem com uma série de arquivos de exemplo macro domínio que você pode usar para seu próprio modelo.

Se você salvou o arquivo de macro como de domínio */ Usr/share/sendmail.cf/domain/vbrew.m4*, Você pode incluir definições em sua *sendmail.mc* por meio de:

```
DOMAIN (`vbrew)
```

RECURSO

A *RECURSO* macro permite que você inclua predefinidos `sendmail` apresenta em sua configuração. Estes `sendmail` características tornam o suporte configurações muito simples de usar. Há um grande número, e ao longo deste capítulo vamos falar sobre apenas alguns dos mais úteis e importantes. Você pode encontrar de full-caudas dos recursos disponíveis no *CF* arquivo incluído no pacote de origem.

Para usar qualquer um dos recursos listados, você deve incluir uma linha em seu *sendmail.mc* que se parece com:

```
FEATURE (nome)
```

onde *nome* é substituído pelo nome do recurso. Algumas características tomar um parâmetro opcional. Se você deseja usar algo diferente do padrão, você deve usar uma entrada que se parece com:

```
FEATURE (nome, param)
```

onde *param* é o parâmetro de fornecimento.

Local definições de macro

O padrão `sendmail` arquivos de configuração macro fornecer lotes de ganchos e variáveis com as quais você pode personalizar a sua configuração. Estes são chamados `locais definições de macro`. Muitos deles estão listados na o *CF* arquivo na `sendmail` origem do pacote.

As definições locais macro são geralmente invocadas, fornecendo o nome da macro com um argumento representação do valor que pretende atribuir à variável da macro gerencia. Mais uma vez, vamos explorar algumas das mais comseg locais definições de macro nos exemplos que apresentamos no final do capítulo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Definição de protocolos de transporte de correio

Se você quiser `sendmail` para o transporte de correio em qualquer outro meio de entrega local, deve dizer-lhe que transportas para usar. A `MAILER` macro faz isto muito fácil. A versão atual do `sendmail` suporta uma variedade de protocolos de transporte de correio, alguns dos quais são experimentais, os outros são, provavelmente, raramente utilizado.

Em nossa rede temos o transporte SMTP para enviar e receber e-mail entre os anfitriões em nossa rede de área local, eo transporte UUCP para enviar e receber e-mails do nosso host inteligente. Para isso, nós simplesmente incluir tanto o `smtp` e `uucp` transportes e-mail. A `local` transporte de email está incluído por padrão, mas pode ser definido para clareza, se desejar. Se você estiver incluindo os `smtp` e `uucp` utentes na sua configuração, você deve certifique-se sempre para definir o `smtp` mailer primeiro.

Os mais comumente utilizados os transportes disponíveis para você utilizar o *MAILER* macro são descritos nos seguintes lista:

local

Este transporte inclui tanto o agente de entrega local usado para enviar e-mail na caixa postal dos usuários sobre esta máquina e *prog* mailer usado para enviar mensagens para programas locais. Esse transporte é incluído por padrão.

smtp

Este transporte implementa o Simple Mail Transport Protocol (SMTP), que é o meio mais comum de transporte de correio na Internet. Quando você incluir este tipo de transporte, quatro utentes estão configurados: `smtp` (Básico SMTP), `esmtp` SMTP (Extended), `smtp8` (8bit binário SMTP limpo), e `relé` (Especificamente projetado para gatewaying mensagens entre hosts).

uucp

A *uucp* transporte fornece suporte para dois envelopes: *uucp de idade*, Que é o UUCP tradicional, e *uucp-novo*, que permite que múltiplos destinatários para ser tratado em uma transferência.

usenet

Este mailer lhe permite enviar mensagens de correio diretamente para as redes de notícias da Usenet estilo. Qualquer local de mensagem di-
corrigidos para um endereço de *news.group.usenet* serão integradas à rede de notícias para o *news.group* newsgroup.

fax

Se você tiver o software instalado HylaFAX, este mailer lhe permitirá enviar e-mail direto para ele para que você possa construir um gateway de fax por e-mail. Esse recurso é experimental, no momento da escrita e mais informações podem ser obtidas a partir de http://www.vix.com/hylafax/.

Há outros, como o *pop*,*procmail*,*mail11*,*phquery*E *cyrus* que são úteis, mas são menos comuns. Se a sua curiosidade é aguçada, você pode ler sobre isso no livro sendmail ou a documentação fornecida na fonte pacote.

Configurar o roteamento de email para hosts locais

A configuração da Cervejaria Virtual é provavelmente mais complexa do que a maioria dos sites exige. A maioria dos sites hoje seria
usar o transporte SMTP somente e não ter de lidar com o UUCP em tudo. Em nossa configuração temos configurado um "Smart host" que é usado para tratar todos os emails enviados. Como estamos usando o transporte SMTP na nossa rede local-trabalho que deve dizer `sendmail` que não é local para enviar e-mail através do host inteligente. A `LOCAL_NET_CONFIG` macro permite-lhe regras sendmail inserir diretamente na saída *sendmail.cf* para modificar a maneira que o correio local é manipulados. Falaremos mais sobre reescrever as regras mais adiante, mas para o momento em que você deve aceitar que a regra que temos
fornecida em nosso exemplo especifica que qualquer e-mail destinado aos sistemas na *vbrew.com* domínio deve ser entregue diretamente ao destino hosts utilizando o transporte de email SMTP.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Gerando o arquivo sendmail.cf

Quando tiver concluído a edição de seu `m4` arquivo de configuração, você deve processá-lo para produzir o */ Etc / mail / sendmail.cf* arquivo lido por `sendmail`. Isso é simples, como ilustrado pelo seguinte exemplo:

```
#  cd / etc / mail
#  m4 / usr/share/sendmail.cf/m4/cf.m4 sendmail.cf> vstout.uucpsmtp.mc
```

Este comando invoca o `m4` processador de macros, fornecendo-lhe o nome de dois arquivos de definição de macro processo. `m4` processa os arquivos na ordem dada. O primeiro arquivo é uma norma `sendmail` modelo macro fornecido com o `sendmail` pacote fonte, a segunda, é claro, é o arquivo que contém a nossa própria definição de macro. A saída do comando é direcionado para o */ Etc / mail / sendmail.cf* arquivo, que é o nosso arquivo de destino.

Você pode começar agora `sendmail` com a nova configuração.

Interpretação e Escrita Regras de Reescrita

Indiscutivelmente a característica mais poderosa de `sendmail` é a regra de reescrita. Reescrever regras são usadas por `sendmail` para determinar como processar uma mensagem de email recebido. `sendmail` passa os endereços da *cabeçalhos* de um e-mail mensagem através de conjuntos de regras de reescrita chamado *rulesets* As regras de reescrita transformar um endereço de e-mail de um forma para a outra e você pode considerá-los como sendo semelhante a um comando em seu editor de texto que substitui todas as correspondam a um padrão especificado por outro.

Cada regra tem um lado esquerdo e lado direito, separados por pelo menos um caracter de tabulação. Quando `sendmail` é de processamento de correio que varre as regras reescrever procurando uma correspondência do lado esquerdo. Se um endereço corresponde ao lado esquerdo de uma regra de reescrita, o endereço é substituído pelo lado direito e processado novamente.

sendmail.cf Comandos de R e S

Na *sendmail.cf* arquivo, os conjuntos de regras são definidas usando comandos codificados como S*n*, Onde *n* especifica o conjunto de regras que está considerado o atual.

As regras se aparecem nos comandos codificados como R. À medida que cada R comando é lido, ele é adicionado à corrente conjunto de regras.

Se você está lidando apenas com o *sendmail.mc* arquivo, você não precisa se preocupar com S comandos em tudo, como as macros construirá aqueles para você. Você terá que manualmente o seu código R regras.

A`sendmail` conjunto de regras, portanto, algo parecido com:

```
Sn
Rrhs lhs
Rlhs2 rhs2
```

Algumas definições úteis Macro

`sendmail` utiliza uma série de definições de macro padrão internamente. O mais útil destes, por escrito, rulesets são:

$ J

O nome de domínio totalmente qualificado do host.

$ W

O componente do nome do host do FQDN.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

$ M

O componente de nome de domínio do FQDN.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Podemos incorporar essas definições macro em nossas regras de reescrita. Nosso Virtual configuração Cervejaria usa o `$ M` macro.

O lado esquerdo

No lado esquerdo de uma regra de reescrita, você pode especificar um padrão que irá corresponder a um endereço que você deseja transformar.

A maioria dos personagens são correspondidos literalmente, mas há uma série de personagens que têm um significado especial, que são descrito na lista a seguir. As regras de reescrita para o lado esquerdo são:

`$ @`

Corresponder exatamente zero tokens

`$ *`

Combina com zero ou mais tokens

`$ +`

Corresponder a um ou mais tokens

`$ -`

Corresponder exatamente um token

`$ =`*x*

Menor frase qualquer na sala de aula *x*

`$ ~`*x*

Match qualquer palavra não em sala de aula *x*

Um token é uma seqüência de caracteres delimitada por espaços. Não há nenhuma maneira de incluir espaços em um sinal, nem é necessário, como os padrões de expressão são flexíveis o suficiente para contornar essa necessidade. Quando uma regra corresponde a um endereço, o texto correspondente a cada um dos padrões na expressão serão atribuídos a variáveis especiais que vamos usar na do lado direito. A única exceção a isso é o `$ @`, Que corresponde a nenhum símbolo e, portanto, não gerará comeram o texto a ser usado no lado direito.

Do lado direito

Quando o lado esquerdo de uma regra de reescrita corresponde a um endereço, o texto original é suprimido e substituído pelo lado direito da regra. Todas as fichas no lado direito são copiados literalmente, a menos que eles começam com um dólar sinal. Assim como para o lado esquerdo, uma série de metasímbolos pode ser usado no lado direito. Tratam-se de descrito na lista a seguir. As regras de reescrita para o lado direito são:

`$`*n*

Este metasymbol é substituído pelo *n*"Expressão ª do lado esquerdo.

`$ [`*nome*`$]`

Este metasymbol resolve hostname nome canônico. Ela passa a ter a forma canônica do hospedeiro nome fornecido.

`$ (`*chave mapa* `$ @`*argumentos* `$:`*padrão* `$)`

Esta é a forma mais geral da pesquisa. A saída é o resultado de olhar para cima *chave* no mapa do chamado *mapa* passando *argumentos* como argumentos. A *mapa* pode ser qualquer um dos mapas que `sendmail` apoia tais como o `virtusertable` que nós descrevemos um pouco mais tarde. Se a pesquisa for bem sucedida, *padrão* será saída. Se um padrão não é fornecido e pesquisa falhar, a entrada é inalterado e *chave* é a saída.

`$>`*n*

Isso fará com que o resto da linha para ser analisado e, em seguida, dado conjunto de regras *n* para avaliar. A saída do conjunto de regras chamada será escrita como saída a esta regra. Este é o mecanismo que permite que as regras para chamar outros rulesets.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`$ #remetente`

Este metasymbol causas avaliação das regras para deter e especifica o mailer que deve ser usado para transporto esta mensagem na próxima etapa da sua entrega. Este metasymbol deve ser chamado somente de 0 conjunto de regras
ou um dos seus sub-rotinas. Esta é a fase final da análise de endereço e deve ser acompanhada pela próximos dois metasímbolos.

`$ @host`

Este metasymbol especifica o host que esta mensagem será enviada ao. Se o host de destino é o host local, ele pode ser omitido. A *host* Pode ser uma lista separada por dois pontos dos anfitriões destino que será em seqüência para entregar a mensagem.

`$:`*usuário*

Este metasymbol especifica o usuário-alvo para a mensagem de email.

A regra de reescrita que corresponde normalmente tentou várias vezes até que ele não corresponder, então a análise passa para a próxima
regra. Esse comportamento pode ser alterado pelo anterior do lado direito com um dos dois lado direito especial metaymbols descritas na lista a seguir. As regras de reescrita de um lado do lado direito metasímbolos controle de circuito são:

`$ @`

Isso faz com que o conjunto de regras metasymbol voltar com o resto do lado direito como o valor. Não outras regras, o conjunto de regras são avaliadas.

`$:`

Isso faz com que metasymbol esta regra para terminar imediatamente, mas o resto do conjunto de regras atual é avaradas.

Um exemplo de padrão simples regra

Para ver melhor como os padrões de substituição de macro funcionar, considere o lado esquerdo seguinte regra:

```
$ * <$ +>
```

Esta regra corresponde a zero ou mais tokens, seguido do caractere <, seguido por um ou mais fichas, seguido pelo caráter> ".

Se essa regra fosse aplicada a `brewer@vbrew.com` ou `Brewer cabeça> <`, A regra não teria partida. O primeiro seqüência não corresponde, porque não incluir um caractere <, ea segunda seria um fracasso, pois `$ +` jogos *um ou mais* fichas e não há sinais entre os <> caracteres. Em qualquer caso em que a regra não partida, do lado direito da regra não é usada.

Se a regra fosse aplicada a `Chefe Brewer <brewer@vbrew.com>`, A regra jogo, e na lado direito `$ 1` seriam substituídos por `Chefe Brewer` e `$ 2` seriam substituídos por `brewer@vbrew.com`.

Se a regra fosse aplicada a `<Brewer@vbrew.com>` a regra seria jogo porque `$ *` jogos *zero* ou mais tokens, e do lado direito `$ 1` seria substituído por uma string vazia.

Conjunto de regras semânticas

Cada um dos `sendmail` conjuntos de regras é chamado a executar uma tarefa diferente no processamento de correio. Quando você está
regras de escrita, é importante entender o que cada um dos conjuntos de regras são esperadas para fazer. Nós vamos olhar para cada um dos
conjuntos de regras que o `m4` scripts de configuração nos permite modificar:

LOCAL_RULE_3

Ruleset 3 é responsável por converter um endereço em um formato arbitrário em um formato comum que `sendmail` será então o processo. O formato de saída esperada é o familiar procura *parte local@host-domain-spec*.

Ruleset 3 deve colocar a parte nome do host do endereço convertido dentro da < e > personagens para fazer a análise

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

mais tarde por conjuntos de regras mais fácil. Ruleset 3 é aplicada antes `sendmail` faz qualquer outra transformação de um endereço de e-mail, de forma

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

se você quiser `sendmail` para o correio de gateway de algum sistema que utiliza alguns formato de endereço incomum, você deve
adicionar uma regra usando o `LOCAL_RULE_3` macro para converter os endereços para o formato comum.

LOCAL_RULE_0 e LOCAL_NET_CONFIG

0 conjunto de regras é aplicado para os endereços dos destinatários por `sendmail` após Ruleset 3. A `LOCAL_NET_CONFIG` macro
regras faz com que seja inserido no *metade inferior* Conjunto de Regras de 0.

0 conjunto de regras é esperado para realizar a entrega da mensagem ao destinatário, por isso deve ser resolvido para um triplo que
especifica cada uma das mailer, host e usuário. As regras serão colocadas antes de qualquer definição de host inteligente pode incluem, portanto, se você adicionar regras que resolvem os endereços corretamente, qualquer endereço que corresponde a uma regra não será han-
dled pelo host inteligente. Esta é a forma como lidamos com a direta `smtp` para os usuários da nossa rede local, no nosso exemplo.

LOCAL_RULE_1 e LOCAL_RULE_2

Um conjunto de regras é aplicado a todos os endereços do remetente e Ruleset 2 é aplicado a todos os endereços dos destinatários. Ambos são
geralmente vazia.

Interpretando a regra em nosso exemplo

Nossa amostra em Exemplo de 18,3 uses do `LOCAL_NET_CONFIG` macro para declarar uma norma local que assegura que qualquer
e-mail dentro do nosso domínio é entregue diretamente com o `smtp` Mailer. Agora que nós olhamos como regras de reescrita são construídas, poderemos compreender como essa regra funciona. Vamos tomar um outro olhar para ele.

Regra de Rewrite vstout.uucpsmtp.m4 Exemplo: 18,3

```
LOCAL_NET_CONFIG
# Esta regra garante que toda a correspondência é entregue local usando o
# Transporte SMTP, tudo o resto vai passar pelo host inteligente.
R $ * <* @ $ $. M. > $ *      smtp $ # $ @ $ 2 $. m. $:. $ 1 <@ $ 2 $ m. > $ 3
```

Nós sabemos que o `LOCAL_NET_CONFIG` macro fará com que a regra a ser inserido em algum lugar perto do fim
ruleset 0, mas antes de qualquer definição de host inteligente. Sabemos também que 0 é o conjunto de regras conjunto de regras último a ser executado e
que ele deve resolver a um três-tupla mailer especificando o usuário, e de acolhimento.

Podemos ignorar as duas linhas de comentário, pois eles não fazem nada de útil. A regra em si é a linha que começa com `R`.
Nós sabemos que o `R` é uma `sendmail` comando e que ele adiciona essa regra para o conjunto de regras actuais, neste caso, conjunto de regras
`0`. Vamos olhar para o lado esquerdo eo lado direito, por sua vez.

O lado esquerdo se parece com: `$ * <* @ $ $. M. > $ *`.

Ruleset 0 espera caracteres <e>, pois é alimentada por três regras. Ruleset 3 converte endereços em comum
forma e para fazer a análise mais fácil, ele também coloca a parte de host do endereço de correio dentro de <> s.

Esta regra corresponde a qualquer endereço de email que parece: `"DestUser <@ somehost.ourdomain. > Alguns Texto '`. Isto é, ele corresponde mail para qualquer usuário em qualquer host dentro do nosso domínio.

Vocês devem lembrar que o texto correspondente metasímbolos do lado esquerdo de uma regra de reescrita é atribuída a definições de macro para o uso do lado direito. No nosso exemplo, o primeiro `$ *` todos os jogos de texto a partir do início do endereço até o caractere <. Todo este texto é atribuído a `$ 1` para uso no lado direito. Da mesma forma o segundo `$ *` em nossa regra de reescrita é atribuída a `$ 2`Eo último é atribuído a `$ 3`.

Agora temos o suficiente para entender o lado esquerdo. Esta regra corresponde mail para qualquer usuário em qualquer host dentro do nosso
domínio. Ele atribui o nome de usuário e US $ 1, o nome de `$ 2`E qualquer texto final a `$ 3`. O lado direito é, então,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

invocada para processar esses.

Vamos agora olhar para o que estamos esperando para ver o output. O lado direito do nosso exemplo rewrite parece como: `smtp $ # $ @ $ 2 $. m. $:. $ 1 <@ $ 2 $ m. > $ 3`.

Quando o lado direito do nosso conjunto de regras é processado, cada um dos metasímbolos são interpretados e relevantes substi-
ções são feitas.

A `$ #` metasymbol causas desta regra para resolver a um envelope específico, *smtp* em nosso caso.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A `$ @` resolve o host de destino. No nosso exemplo, o host de destino é especificado como `$ 2 $. M.`, Que é o totalmente quali-
cados nome de domínio do host em nosso domínio. O FQDN é construído do componente hostname atribuído para `$ 2` do nosso lado esquerdo com o nosso nome de domínio (`. $ M.`) Anexado.

A `$:` metasymbol especifica o usuário-alvo, que mais uma vez capturada a partir do lado esquerdo e tinha armazenado em `$ 1`.

Preservamos o conteúdo da seção de <>, e todo o texto à direita, usando os dados foram coletados a partir do lado esquerdo lado da regra.

Uma vez que esta regra resolve um mailer, a mensagem é encaminhada para o mailer para entrega. No nosso exemplo, o mes-sábio seria encaminhado para o host de destino usando o protocolo SMTP.

Configurando as opções do sendmail

`sendmail` tem um número de opções que permitem personalizar a forma como ele executa determinadas tarefas. Há um grande número desses, por isso listamos apenas alguns dos mais comumente usados na lista de futuros.

Para configurar qualquer uma dessas opções, você pode ou defini-los na `m4` arquivo de configuração, que é a prefe-
método capaz, ou você pode inseri-los diretamente no *sendmail.cf* arquivo. Por exemplo, se quiséssemos ter `Enviar-e-mail` garfo um novo emprego para cada mensagem de correio para ser entregue, podemos acrescentar a seguinte linha para o nosso `m4` configu-
ficheiro de ração:

```
define (`confSEPARATE_PROC ',' true ')
```

O correspondente *sendmail.cf* entrada criada é:

```
O ForkEachJob = true
```

A lista a seguir descreve comum *sendmail m4* opções (e *sendmail.cf* equivalentes):

`confMIN_FREE_BLOCKS (MinFreeBlocks)`

Há ocasiões em que um problema pode impedir a entrega imediata de mensagens de correio, causando mensagens a fila no spool de email. Se o seu host de correio processos de grandes volumes de e-mail, é possível para o spool de email a crescer para um tamanho que enche o sistema de arquivos de suporte da bobina. Para evitar isso, `sendmail` fornece esta opção para especificar o número mínimo de blocos de disco livre que deve existir antes de uma mensagem de correio será ac-
ahead of print. Isto permite-lhe garantir que `sendmail` nunca faz com que seu sistema de ficheiros de spool para ser preenchido (padrão: 100).

`confME_TOO (METOO)`

Quando um alvo de email, como um alias de e-mail é expandida, às vezes é possível que o remetente pode aparecer no lista de destinatários. Esta opção determina se os autores de uma mensagem de e-mail receberá uma cópia se aparecem na lista de destinatários expandida. Os valores válidos são "verdadeiros" e "falso" (Padrão: false).

`confMAX_DAEMON_CHILDREN (MaxDaemonChildren)`

Sempre `sendmail` recebe uma ligação SMTP entre um host remoto, ele gera uma nova cópia de si mesmo para lidar com a mensagem de e-mails recebidos. Dessa forma, é possível que `sendmail` a transformação múltipla entrada mensagens de correio simulatanenously. Embora isso seja útil, cada nova cópia do `sendmail` consome memória no computador host. Se um número invulgarmente elevado de conexões de entrada são recebidos, por acaso, por causa de um problema ou um ataque mal-intencionado, é possível que `sendmail` daemons para consumir toda a memória do sistema. Esta op-
ção fornece-lhe um meio de limitar o número máximo de crianças daemon que será gerado.
Quando este número for atingido, novas conexões são rejeitadas até que algumas das crianças existentes têm denunciado (Padrão: indefinido).

`confSEPARATE_PROC (ForkEachJob)`

Ao processar a fila de emails e mensagens de correio a enviar, `sendmail` processos de uma mensagem de correio de cada vez. Quando esta opção for ativada, `sendmail` bifurcará uma nova cópia de si mesmo para cada mensagem a ser entregue. Esta é particularmente útil quando existem algumas mensagens de email que estão presos na fila por causa de um problema com o host de destino (Padrão: false).

`confSMTP_LOGIN_MSG (SmtpGreetingMessage)`

Sempre que uma ligação é feita para `sendmail`, Uma mensagem de saudação é enviada. Por padrão, essa mensagem contém a

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

hostname, nome do agente de transferência de correio, o número da versão do sendmail, o número da versão local, e os cur-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

aluguel de data. RFC821 especifica que a primeira palavra da saudação deve ser o nome de domínio totalmente qualificado do hospedeiro, mas o resto da saudação podem ser configurados como desejar. Você pode especificar macros sendmail aqui e que será ampliado quando usado. As únicas pessoas que vão ver essa mensagem está sofrendo administração do sistema tradores diagnosticar problemas de entrega de email ou fortemente curiosos interessados em descobrir como a máquina está configurado. Você pode aliviar um pouco do tédio de suas funções, personalizando a mensagem de boas vindas com algumas
witticisms; ser agradável. A palavra "EMSTP" será inserido entre as palavras, primeiro e segundo por `sendmail`, Como este é o sinal para hosts remotos que suportam o protocolo ESMTP (Padrão: `$ J Sendmail v $ / $ Z; $ b`).

Algumas configurações de sendmail úteis

Existe uma infinidade de possíveis `sendmail` configurações. Neste espaço, vamos ilustrar apenas alguns tipos importantes de configuração que será útil em muitas `sendmail` instalações.

Confiando usuário definir o campo From:

Às vezes é útil para substituir o `De:` campo de uma mensagem de correio de saída. Digamos que você tenha um web-programa baseado que gera e-mail. Normalmente, a mensagem de email que parece vir do usuário que pertence o processo do servidor web. Podemos querer especificar algum endereço de outra fonte, para que o e-mail parece ter originado de algum outro usuário ou o endereço em que máquina. `sendmail` fornece um meio de especificar quais usuários dos sistemas são confiadas com a capacidade de fazer isso.

A `use_ct_file` recurso permite a especificação e uso de um arquivo que lista os nomes de usuários confiáveis. Por padrão, um pequeno número de usuários do sistema são confiáveis `sendmail` (`root`, Por exemplo). O nome de arquivo padrão
para esta função é */ Etc / mail / trusted-users* em sistemas de exploração da */ Etc / mail /* diretório de configuração e */ Etc / sendmail.ct* naqueles que não. Você pode especificar o nome ea localização do arquivo, substituindo o `confCT_FILE` definição.

Adicionar FEATURE (use_ct_file) para o seu *sendmail.mc* arquivo para habilitar o recurso.

Gerenciando Alias Mail

aliases de correio são um poderoso recurso que permite e-mail para ser direcionado às caixas de correio que são nomes

alternativos para os usuários
ou processos em um host de destino. Por exemplo, é prática comum ter feedback ou comentários relativos a um servidor de World Wide Web para ser direcionado para "webmaster". Muitas vezes não é um usuário conhecido como "webmaster" na
máquina de destino, em vez disso, é um apelido de outro usuário do sistema. Outro uso comum dos mail alias é explorado por programas de correio servidor de listas em que um alias direciona as mensagens de entrada para o programa servidor de listas para o manuseio.

A */ Etc / aliases* arquivo é onde são armazenados os apelidos. A `sendmail` programa de consulta esse arquivo para determinar como lidar com uma mensagem de correio de entrada. Se ele encontra uma entrada neste arquivo correspondente ao usuário alvo no e-mail
mensagem, ele redireciona a mensagem para onde a entrada descreve.

Especificamente, há três coisas que alias permitir que aconteça:

- Eles fornecem uma forma abreviada ou o nome bem conhecido por e-mail para ser dirigida para ir a um ou mais pessoas.
- Eles podem chamar um programa com a mensagem de correio como a entrada para o programa.
- Eles podem enviar email para um arquivo.

Todos os sistemas necessitam pseudônimos para *Postmaster* e *MAILER DAEMON*- para ser compatível com RFC.

Sempre estar extremamente conscientes de segurança quando da definição aliases que invocar programas ou gravar programas,

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

desde
`sendmail` geralmente é executado com *root* permissões.

Detalhes sobre aliases de correio podem ser encontrados no *aliases (5)* manual de página. Uma amostra de *aliases* arquivo é

mostrado em
Exemplo de 18,4.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

18,4 Exemplo: Exemplo de arquivo aliases

```
#
# Os dois seguintes aliases devem estar presentes para ser compatível com RFC.
# É importante para resolvê-los de "uma pessoa que lê e-mail de forma rotineira.
#
postmaster:    root                            # Entrada requerida
MAILER-DAEMON: postmaster                      # Entrada requerida
#
#
# Demonstrar os tipos mais comuns de apelidos
#
usenet:        janet                           # alias para uma pessoa
admin:         joe, janet                      # alias para várias pessoas
newspak usuários:: include: / usr / lib / listas / newspak # ler os destinatários a
partir do arquivo
changefeed:    | / Usr / local / gup / lib     # Alias que invoca o programa
queixas:       / Var / log / reclamações       alias # escreve e-mail para arquivo
#
```

Sempre que você atualizar o */ Etc / aliases* arquivo, certifique-se de executar o comando:

```
# / Usr / bin / newaliases
```

para reconstruir o banco de dados que `sendmail` usa internamente. A `/ Usr / bin / newaliases` comando é uma simbólica
link para o `sendmail` executável, e quando chamado desta forma, se comporta exatamente como se fosse invocada como:

```
# / Usr / lib / sendmail-bi
```

A `newaliases` comando é uma alternativa e maneira mais conveniente de fazer isso.

Usando um host inteligente

Às vezes, um hospedeiro encontra-mail que é incapaz de entregar diretamente para o host remoto desejado. Muitas vezes é

conveniente
ter um único host em uma rede de assumir o papel de gerenciar a transmissão de e-mail para hosts remotos que são
de difícil acesso, ao invés de ter cada host local tentar fazer isso de forma independente.

Existem algumas boas razões para ter um único hospedeiro assumir a gestão do correio. Você pode simplificar o gerenciamento

de
Tendo apenas uma máquina com uma configuração de e-mail completo que sabe como lidar com todos os diferentes mail
tipos de transporte, tais como UUCP, Usenet, etc Todos os outros hosts só precisa de um protocolo único tranport para enviar
seu e-mail
para esta máquina central. Hosts que enchem este e-mail central de roteamento e encaminhamento de papel são chamados *hosts inteligentes.* Se você tem
um host inteligente que irá aceitar e-mail de você, você pode enviar e-mail de qualquer espécie e que irá gerenciar o roteamento
e
transmissão de e-mail para que os destinos pretendidos remoto.

Outra boa aplicação para configurações de host inteligente é gerenciar a transmissão de e-mail através de um fogo privado parede. Uma organização pode optar por instalar uma rede de IP privado e utilizar os seus próprios endereços IP privativos. A rede privada pode ser conectado à Internet através de um firewall. Enviando e-mails para e de hosts no pri-
redes privadas para o exterior usando o SMTP não seria possível em uma configuração convencional, pois
as máquinas não são capazes de aceitar ou estabelecer conexões de rede direta para hosts na Internet. Em vez disso, a ou-
nização pode optar por ter o firewall oferecem uma função mail host inteligente. O host inteligente em execução no
firewall é capaz de estabelecer conexões de rede direta com os hosts da rede privada e na Inter-
net. O host inteligente aceitaria mail de ambos os hosts da rede privada ea Internet, armazená-los em
armazenamento local e depois gerir a retransmissão de e-mail para o host correto diretamente.

Smart hosts são normalmente usadas quando todos os outros métodos de entrega fracassaram. No caso da organização com a rede privada, seria perfeitamente razoável para que os anfitriões tentam entregar mensagens diretamente em primeiro lugar, e se isso falhar, então enviá-lo para o host inteligente. Isso alivia o host inteligente de um lote de tráfego, porque os outros hosts pode enviar e-mail diretamente para outras máquinas na rede privada.

`sendmail` fornece um método simples de configurar um host inteligente usando o `SMART_HOST` recurso, quando im-
mentação que na configuração Cervejaria Virtual, nós fazemos exatamente isso. As partes relevantes da nossa configuração
arquivo definem o host inteligente são:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
define (`SMART_HOST ',` uucp-novo: moria ")
LOCAL_NET_CONFIG
# Esta regra garante que toda a correspondência é entregue local usando o
# Transporte SMTP, tudo o resto vai passar pelo host inteligente.
R $ * <* @ $ $. M. > $ *  smtp $ # $ @ $ 2 $. m. $:. $ 1 <@ $ 2 $ m. > $ 3
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A SMART_HOST macro permite que você especifique o host que deverá retransmitir todas as mensagens de saída que você é incapaz
para entregar diretamente, eo protocolo de transporte de correio para usar para falar com ele.

Em nossa configuração, estamos usando o uucp-novo transporte para hospedar UUCP moria. Se quisermos configurar sendmail usar um baseado em SMTP Host Inteligente, teríamos, em vez de usar algo como:

```
define (`SMART_HOST ',` mail.isp.net)
```

Nós não precisamos especificar SMTP como o transporte, como é o padrão.

Você consegue adivinhar o que o LOCAL_NET_CONFIG macro e reescrever a regra poderia estar fazendo?

A LOCAL_NET_CONFIG macro permite que você adicione-primas sendmail reescrever as regras para sua configuração que definir o e-mail deve ficar dentro do sistema de correio local. No nosso exemplo, usamos uma regra que combina com qualquer e-mail onde o anfitrião pertence ao nosso domínio (. $ M.) E reescrevê-lo para que seja enviada diretamente para o SMTP Mailer. Isso garante que qualquer mensagem para um host em nosso domínio local é direcionado imediatamente para o mailer SMTP
e encaminhados para o anfitrião, ao invés de cair meio ao nosso host inteligente, que é o tratamento padrão.

Gerenciando e-mails indesejados ou não solicitados (spam)

Se você se inscreveu para uma mailing list, publicado o seu endereço de e-mail em um web site, ou postou um artigo na Usenet, você provavelmente já começaram a receber e-mails publicitários não solicitados. É comum agora para as pessoas vasculhar a rede em busca de endereços de e-mail para adicionar à lista de discussão que, depois, vender para empresas que buscam ad-
vertise seus produtos. Este tipo de comportamento de envio em massa é comumente chamado de "spam".

O dicionário gratuito on-line de Informática oferece uma definição-mail específico de spam como:[112]

2. (A redução do sentido 1, acima) indiscrimately Para enviar grandes quantidades de correio electrónico não solicitado

destinado a promover
um produto ou serviço. Spam neste sentido é algo como o equivalente eletrônico de lixo enviado ao "ocupante".

Na década de 1990, com o aumento da consciência comercial da rede, na verdade existem canalhas que oferecem spam como um "serviço" para empresas que desejem anunciar na rede. Eles fazem isso por correio para coleções de e-mail endereços, Usenet News, ou listas de discussão. Estas práticas têm causado indignação e reação agressiva por parte de muitos líquidos
usuários contra os indivíduos em causa.

Felizmente, sendmail inclui suporte para alguns mecanismos que podem ajudar a lidar com e-mails não solicitados.

O Real-time Blackhole List

A Lista Real-time Blackhole é um serviço público previsto para ajudar a reduzir o volume de publicidade não solicitada você tem que enfrentar. Conhecido fontes de e-mail e anfitriões estão listados em um banco de dados passível de consulta na Internet.
Eles entraram lá por pessoas que receberam publicidade não solicitada de algum endereço de email. Major do-
corrente, por vezes, encontram-se na lista por causa de deslizes em encerrar spam. Enquanto algumas pessoas queixam-se nomeadamente sobre as escolhas feitas pelos mantenedores da lista, e continua sendo muito popular e desencontros geralmente são elaborados rapidamente. Detalhes completos sobre como o serviço é operado pode ser encontrada no site da casa Correio do Sistema de Proteção ao Abuso http://maps.vix.com/rbl/.

Se você ativar esta sendmail recurso, ele vai testar o endereço de origem de cada mensagem de e-mails recebidos contra o Real-time Blackhole List para determinar se a aceitar a mensagem. Se você tem um site grande, com muitos usuários, esse recurso poderia economizar um volume considerável de espaço em disco. Este recurso aceita um parâmetro para especificar o nome
do servidor para o uso. O padrão é o servidor principal em *rbl.maps.vix.com*.

Para configurar o recurso Lista de Real-time Blackhole, adicione a seguinte declaração macro para o seu *sendmail.mc* arquivo:

```
FEATURE (RBL)
```

Se desejar especificar algumas servidor RBL outro, você poderia usar uma declaração como esta:

```
FEATURE (RBL, rbl.host.net »)
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

112 A Free On-Line Dictionary of Computing pode ser encontrada embalada em muitas distribuições Linux, ou on-line em sua página pessoal em http://wombat.doc.ic.ac.uk/foldoc/.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O banco de dados de acesso

Um sistema alternativo que oferece maior flexibilidade e controle no custo de configuração manual é o `Enviar-e-mail` *access_db* característica. O banco de dados de acesso permite que você configure os hosts ou usuários que você aceitará mail e de que você irá fazer relay de correio para.

Gerenciando que você vai para a retransmissão de email é importante, pois é uma outra técnica comumente empregada por meio

de spam
hosts para burlar sistemas, como a Lista Real-time Blackhole acabamos de descrever. Em vez de enviar o email para diretamente, os spammers relay de mensagens através de algum outro host incautos que permite isso. O SMTP de entrada conexão, em seguida, não vem do hospedeiro de spam conhecidas, em vez vem do host de retransmissão. Para assegurar que os seus anfitriões e-mail próprio não são usados dessa maneira, você deve retransmissão de email apenas para máquinas conhecidas. Versões do `Enviar-e-mail` que são 8.9.0 ou mais recentes têm afinação desativado por padrão, então para aqueles que você precisa usar o acesso a dados
base para permitir que hosts individuais para retransmissão.

A idéia geral é simples. Quando uma nova conexão SMTP é recebida, `sendmail` recupera o mes-
informações de cabeçalho e sábio então consulta o banco de dados de acesso para ver se ele deve proceder para aceitar a corpo da mensagem em si.

O banco de dados de acesso é um conjunto de regras que descrevem o que deveriam ser tomadas medidas para as mensagens

recebidas de
nomeado hosts. O padrão de arquivo de controle de acesso é chamado */ Etc / mail / access*. A tabela tem um formato simples. Cada
linha da tabela contém uma regra de acesso. O lado esquerdo de cada regra é um padrão usado para combinar com o remetente de uma
mensagem de correio de entrada. Pode ser um endereço completo, nome de host ou um endereço IP. O lado direito é as medidas a tomar. Existem cinco tipos de ação, você pode configurar. São eles:

OK

Aceite a mensagem de email.

RELAY

Aceitar mensagens a partir deste host ou usuário, mesmo se eles não estão destinados para o nosso host, isto é, aceitar-

show
sábios para a transmissão para outros hospedeiros deste acolhimento.

REJECT

Rejeitar o e-mail com uma mensagem genérica.

DESCARTE

Descartar a mensagem usando a `$ # Descartar` Mailer.

Qualquer texto

Retorna uma mensagem de erro usando # # # como o código de erro (que deve ser compatível com RFC-821) e

"qualquer
texto "como a mensagem.

Um exemplo */ Etc / mail / access* pode parecer:

```
friends@cybermail.com   REJECT
aol.com                 REJECT
207.46.131.30           REJECT
postmaster@aol.com      OK
linux.org.au            RELAY
```

Este exemplo rejeitaria qualquer e-mail recebido de *friends@cybermail.com*, Qualquer host no domínio aol.com e de acolhimento 207.46.131.30. A próxima regra aceitaria e-mail de *postmaster@aol.com* apesar do fato de que o domínio em si tem um rejeitam regra. A última regra permite a retransmissão de correio a partir de qualquer host na linux.org.au domínio.

Para habilitar o recurso de banco de dados de acesso, uso a seguinte declaração em seu *sendmail.mc* arquivo:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`FEATURE (access_db)`

A definição padrão cria o banco de dados usando `hash-o / etc / mail / access`, O que gera uma simples banco de dados de hash do arquivo de texto simples. Isto é perfeitamente adequada na maioria das instalações. Há outras opções que você deve considerar se você pretende ter um acesso de dados de grande porte. Consulte o *sendmail* livro ou outro `sendmail` documentação para mais detalhes.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Exceto que os usuários recebam e-mail

Se você tiver usuários ou processos automatizados que enviar e-mail, mas não há necessidade de recebê-lo, às vezes é útil recusar-se a aceitar e-mails destinados a eles. Isso economiza espaço em disco desperdiçado mail de armazenamento de que nunca serão lidos. A
blacklist_recipients recurso, quando utilizado em combinação com o *access_db* recurso, permite que você desabilite a recebimento de e-mail para usuários locais.

Para habilitar o recurso, você adiciona as seguintes linhas ao seu *sendmail.mc* arquivo, se eles não estiverem lá:

```
FEATURE (access_db)
FEATURE (blacklist_recipients)
```

Para desativar o recebimento de e-mail para um usuário local, basta adicionar os seus dados no banco de dados de acesso.

Normalmente você usaria
o # # # O modelo de entrada que retorna uma mensagem de erro significativa para o remetente para que eles saibam por que o email não é
sendo entregue. Esse recurso se aplica igualmente bem para usuários em domínios de correio virtual, e você deve incluir o domínio de correio virtual na especificação do banco de dados de acesso. Algumas amostras */ Etc / mail / access* entradas pode parecer:

```
daemon          550 Daemon não aceitar ou não ler e-mails.
Flacco          550 Mail para este usuário está desativada administrativamente.
grump@dairy.org 550 Mail desativado para este destinatário.
```

Configurando Email Virtual Hosting

Virtual e-mail de hospedagem oferece um anfitrião a capacidade de aceitar e entrega do correio em nome de uma série de diferentes domínios, como se fosse um número de hosts e-mail separado. Mais comumente, hospedagem virtual é ex-breexplotadas pela Internet Application em associação com provedores de web hosting virtual, mas é simples de configurar e você nunca sabe quando poderia estar em posição de receber uma lista de discussão virtual para o seu projeto Linux favorita, então vamos descrevê-lo aqui.

Aceitando-mail para outros domínios

Quando `sendmail` recebe uma mensagem de e-mail, ele compara o host de destino nos cabeçalhos de mensagens para o nome do host local. Se forem iguais, `sendmail` aceita a mensagem para entrega local, se eles diferem, `sendmail` pode decidir aceitar a mensagem e tentar enviá-lo para o destino final (ver "O banco de dados de acesso" anteriormente neste capítulo para obter detalhes sobre como configurar `sendmail` para aceitar e-mail para encaminhamento).

Se quisermos configurar hospedando emails virtuais, a primeira coisa que precisamos fazer é convencer `sendmail` que deve também aceitar mensagens para os domínios que estamos hospedando. Felizmente, isso é uma coisa muito simples de fazer.

A `sendmail` *use_cw_file* recurso nos permite especificar o nome de um arquivo onde armazenar os nomes de domínio para que `sendmail` aceita e-mails. Para configurar o recurso, inclua a declaração de recurso para sua *sendmail.mc* arquivo:

```
FEATURE (use_cw_file)
```

O nome padrão do arquivo será */ Etc / mail / local-host-names* para distribuições usando o */ Etc / mail /* configuração diretório ou */ Etc / sendmail.cw* para aqueles que não. Alternativamente, você pode especificar o nome ea localização do arquivo , substituindo o `confCW_FILE` macro usando uma variação em:

```
define (`confCW_FILE ',` / etc / virtualnames)
```

Para ficar com o nome de arquivo padrão, se quisermos oferecer hospedagem virtual ao bovine.net,dairy.orgE arte ist.org domínios, que criaria uma */ Etc / mail / local-host-names* que se parece com:

```
bovine.net
dairy.org
artist.org
```

Quando isso é feito, e assumindo que existem registros de DNS mais apropriado que ponto esses nomes de domínio para o nosso anfitrião,
`sendmail` aceita mensagens de correio para os domínios, como se fossem destinados a nosso domínio real nome.

Encaminhamento virtual hospedado e-mail para outros destinos

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A `sendmail` *virtusertable* O suporte ao recurso configura para a tabela de usuário virtual, onde configurar virtual e-mail de hospedagem. Os mapas do usuário da tabela virtual e-mails recebidos destinados a alguns *user @ host* para alguns

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

otherhost otheruser @. Você pode pensar nisso como um avançado recurso de alias de correio, que funciona não apenas com o usuário de destino, mas também o domínio de destino.

Para configurar o *virtusertable* recurso, adicionar o recurso para sua *sendmail.mc* configuração, como mostrado:

```
FEATURE (virtusertable)
```

Por padrão, o arquivo que contém as regras para realizar traduções serão */ Etc / mail / virtusertable*. Você pode substituir isso fornecendo um argumento para a definição de macro, consulte um detalhado `sendmail` de referência para saber mais sobre
quais opções estão disponíveis.

O formato da tabela de usuários virtuais é muito simples. O lado esquerdo de cada linha contém um padrão que representa o endereço de destino original, do lado direito tem um padrão que representa o endereço de correio virtual
hospedado endereço será mapeado.

O exemplo a seguir mostra três possíveis tipos de entradas:

```
samiam@bovine.net      colin
sunny@bovine.net       darkhorse@mystery.net
@ Dairy.org            mail@jhm.org
@ Artist.org           $ 1@red.firefly.com
```

Neste exemplo, estamos a virtual hosting três domínios: bovine.net,dairy.orgE artist.org.

A primeira entrada redireciona mensagens enviadas para um usuário no bovine.net domínio virtual para um usuário local na máquina. A
segunda entrada redireciona e-mail para um usuário no mesmo domínio virtual para um usuário em outro domínio. O terceiro exemplo
redireciona todos os e-mails endereçados a qualquer usuário no dairly.org domínio virtual para um endereço de e-mail único controle remoto. Finalmente,
a última entrada redireciona qualquer e-mail para um usuário no artist.org domínio virtual para o mesmo usuário em outro domínio, por
exemplo, *julie@artists.org* seria redirecionado para *julie@red.firefly.com*.

Testando sua Configuração

A `m4` comando processa os arquivos de definição de macro de acordo com suas regras de sintaxe própria, sem a compreensão nada sobre o correto `sendmail` sintaxe, de modo que não haverá nenhuma mensagem de erro se você chegou nada de errado em seu arquivo de definição de macro. Por esta razão, é muito importante que você teste completamente a sua configuração. Felizmente, `sendmail` fornece uma maneira relativamente fácil de fazer isso.

`sendmail` suporta um "endereço de teste" modalidade que permite testar nossa configuração e identificar eventuais erros. Em Neste modo de operação, nós invocamos `sendmail` a partir da linha de comando, e pede-nos para um conjunto de regras espe-ção e um endereço de e-mail de destino. `sendmail` em seguida, os processos que o endereço de destino com as regras especificadas,
Exibindo a saída de cada regra de reescrita como ela procede. Para colocar `sendmail` para este modo, nós chamá-lo com o `-Bt` argumento:

```
# / Usr / sbin / sendmail-bt
ENDEREÇO MODO DE TESTE (conjunto de regras 3 NÃO invocado automaticamente)
Digite <ruleset> <address>
>
```

O arquivo de configuração padrão utilizado é o */ Etc / mail / sendmail.cf* arquivo, você pode especificar uma configuração alternativa
arquivo usando o `-C` argumento. Para testar nossa configuração, é preciso selecionar um número de endereços de processo que vai dizer-nos que cada um dos nossos requisitos entregando-mail são atendidas. Para ilustrar isso, vamos trabalhar através de um teste da nossa mais complicada a configuração do UUCP mostrado no Exemplo 18.2.

Primeiro vamos testar se `sendmail` é capaz de enviar mensagens para os usuários locais no sistema. Nestes testes esperamos que todos os
endereços que ser reescrito para o local mailer sobre esta máquina:

```
# / Usr / sbin / sendmail-bt
ENDEREÇO MODO DE TESTE (conjunto de regras 3 NÃO invocado automaticamente)
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
Digite <ruleset> <address>
> 3,0 isaac
reescrita: conjunto de regras 3     entrada: isaac
reescrita: conjunto de regras 96    entrada: isaac
reescrita: conjunto de regras 96 retorna: isaac
reescrita: conjunto de regras 3 devolve: Isaque
reescrita: conjunto de regras 0     entrada: isaac
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
reescrita: conjunto de regras 199   entrada: isaac
reescrita: conjunto de regras 199 devolve: Isaque
reescrita: conjunto de regras    98     entrada: isaac
reescrita: conjunto de regras    98 retorna: isaac
reescrita: conjunto de regras 198entrada: isaac
reescrita: conjunto de regras 198 retornos: $ # $ local: isaac
reescrita: conjunto de regras    0 retorna: # $ local $: isaac
```

Este resultado mostra-nos como `sendmail` processos de correspondência dirigida à isaac neste sistema.

Cada linha mostra-nos
que a informação foi fornecida a um conjunto de regras ou o resultado obtido do processamento de um
conjunto de regras. Dissemos
`sendmail` quiséssemos usar conjuntos de regras 3 e 0 a processo o endereço. 0 conjunto de regras é o que normalmente é chamado e
forçamos ruleset 3 porque ele não é testado por padrão. A última linha mostra-nos que o resultado de 0 conjunto de regras não e-mail direto a verdade isaac ao local Mailer.

Em seguida, vamos testar e-mails endereçados para o nosso endereço SMTP: isaac@vstout.vbrew.com. Devemos ser capazes

de produzir
o mesmo resultado final como o nosso último exemplo:

```
# / Usr / sbin / sendmail-bt
ENDEREÇO MODO DE TESTE (conjunto de regras 3 NÃO invocado automaticamente)
Digite <ruleset> <address>
isaac@vstout.vbrew.com> 3,0
reescrita: conjunto de regras 3     entrada: vstout @ isaac. vbrew. com
reescrita: conjunto de regras 96    entrada: <isaac vstout @. vbrew. > Com
reescrita: conjunto de regras 96 retorna: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 3 retorna: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 0     entrada: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 199   entrada: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 199 retorna: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 98    entrada: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 98 retorna: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 198   entrada: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 198 retornos: $ # $ local: isaac
reescrita: conjunto de regras 0 retorna: # $ local $: isaac
```

Novamente, o teste passou. Em seguida, vamos testar o nosso endereço de e-mail para o estilo UUCP: vstout! isaac.

```
# / Usr / sbin / sendmail-bt
ENDEREÇO MODO DE TESTE (conjunto de regras 3 NÃO invocado automaticamente)
Digite <ruleset> <address>
> 3,0 vstout! Isaac
reescrita: conjunto de regras 3     entrada: vstout! isaac
reescrita: conjunto de regras 96    entrada: <isaac vstout @. UUCP>
reescrita: conjunto de regras 96 retorna: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 3 retorna: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 0     entrada: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 199   entrada: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 199 retorna: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 98    entrada: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 98 retorna: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 198   entrada: <isaac vstout @. vbrew. com. >
reescrita: conjunto de regras 198 retornos: $ # $ local: isaac
reescrita: conjunto de regras 0 retorna: # $ local $: isaac
```

Este teste também tem passado. Esses testes confirmam que qualquer e-mail recebido por usuários locais sobre esta máquina será

prop-
Erly entregues independentemente da forma como o endereço é formatado. Se você definiu as alcunhas para sua máquina, como como máquinas virtuais, você deve repetir esses testes para cada um dos nomes alternativos através dos quais esta máquina é conhecida a en-
certeza de que eles também funcionam corretamente.

Em seguida, vamos testar esse e-mail endereçado a outros hosts na vbrew.com domínio é entregue diretamente para o host utilizando o envelope SMTP:

```
# / Usr / sbin / sendmail-bt
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
ENDEREÇO MODO DE TESTE (conjunto de regras 3 NÃO invocado automaticamente)
Digite <ruleset> <address>
isaac@vale.vbrew.com> 3,0
reescrita: conjunto de regras 3     entrada: isaac @ Vale. vbrew. com
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
reescrita: conjunto de regras 96    entrada: <isaac @ Vale. vbrew. > Com
reescrita: conjunto de regras 96 retorna: <isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras    3 retorna: <isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras    0     entrada: <isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras 199entrada: <isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras 199 retorna: <isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras    98    entrada: <isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras    98 retorna: <isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras 198entrada: <isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras 198 retornos: $ smtp # $ @ Vale. vbrew. com. /
    $: <Isaac @ Vale. vbrew. com. >
reescrita: conjunto de regras    0 devolve: $ # $ @ smtp vale. vbrew. com. /
    $: <Isaac @ Vale. vbrew. com. >
```

Podemos ver que este teste tem dirigido a mensagem para o SMTP mailer para ser encaminhado diretamente para a vale.vbrew.com anfitrião e especifica que o usuário isaac. Este teste confirma que a nossa LOCAL_NET_CONFIG definição funciona corretamente. Para esse teste para ter sucesso, o nome do host de destino deve ser capaz de ser resolvido corretamente, por isso
ou deve ter uma entrada no nosso */ Etc / hosts* arquivo, ou em nosso DNS local. Nós podemos ver o que acontece se o destino máquina não é capaz de ser resolvido por intencionalmente especificando um host desconhecido:

```
# / Usr / sbin / sendmail-bt
ENDEREÇO MODO DE TESTE (conjunto de regras 3 NÃO invocado automaticamente)
Digite <ruleset> <address>
isaac@vXXXX.vbrew.com> 3,0
reescrita: conjunto de regras 3     entrada: isaac @ vXXXX. vbrew. com
reescrita: conjunto de regras 96    entrada: isaac <@ vXXXX. vbrew. > Com
Nome do tempo limite do servidor: vXXXX.vbrew.com
reescrita: conjunto de regras 96 devolve: Isaque @ vXXXX. vbrew. > Com
reescrita: conjunto de regras 3 devolve: Isaque @ vXXXX. vbrew. > Com
== Ruleset 3,0 status (3) 75
reescrita: conjunto de regras 0     entrada: isaac <@ vXXXX. vbrew. > Com
reescrita: conjunto de regras 199   entrada: isaac <@ vXXXX. vbrew. > Com
reescrita: conjunto de regras 199 devolve: Isaque @ vXXXX. vbrew. > Com
reescrita: conjunto de regras 98    entrada: isaac <@ vXXXX. vbrew. > Com
reescrita: conjunto de regras 98 devolve: Isaque @ vXXXX. vbrew. > Com
reescrita: conjunto de regras 198   entrada: isaac <@ vXXXX. vbrew. > Com
reescrita: conjunto de regras 95    entrada: <uucp-novo: moria> <isaac /
    @ VXXXX. vbrew. > Com
reescrita: conjunto de regras 95 retorna: $ # uucp-novo $ $ @ moria: <isaac /
    @ VXXXX. vbrew. > Com
reescrita: conjunto de regras 198 retornos: $ # uucp-novo $ $ @ moria: <isaac /
    @ VXXXX. vbrew. > Com
reescrita: conjunto de regras 0 devolve: $ # uucp-novo $ $ @ moria: <isaac /
    @ VXXXX. vbrew. > Com
```

Este resultado é muito diferente. Em primeiro lugar, 3 ruleset retornou uma mensagem de erro, indicando o nome do host não pôde ser re-
resolvido. Em segundo lugar, nós lidamos com esta situação, contando com a outra característica fundamental da nossa configuração, o smart
host. O host inteligente vontade para lidar com qualquer email que é caso contrário não entregues. O nome do host que especificadas no presente
teste foi incapaz de ser resolvido e os conjuntos de regras determinou que o e-mail devem ser enviadas para o nosso host inteligente
moria usando o uucp-novo Mailer. Nosso host inteligente pode ser mais ligado e sabe o que fazer com o ad-
vestido.

Nosso teste final garante que qualquer e-mail endereçado a um host não dentro do nosso domínio é entregue ao nosso host inteligente. Este deve produzir um resultado semelhante ao nosso exemplo anterior:

```
# / Usr / sbin / sendmail-bt
ENDEREÇO MODO DE TESTE (conjunto de regras 3 NÃO invocado automaticamente)
Digite <ruleset> <address>
isaac@linux.org.au> 3,0
reescrita: conjunto de regras 3     entrada: isaac @ linux. org. au
reescrita: conjunto de regras 96    entrada: <isaac @ linux. org. > Au
reescrita: conjunto de regras 96 retorna: <isaac @ linux. org. au. >
reescrita: conjunto de regras 3 retorna: <isaac @ linux. org. au. >
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
reescrita: conjunto de regras 0     entrada: <isaac @ linux. org. au. >
reescrita: conjunto de regras 199   entrada: <isaac @ linux. org. au. >
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
reescrita: conjunto de regras 199 retorna: <isaac @ linux. org. au. >
reescrita: conjunto de regras    98    entrada: <isaac @ linux. org. au. >
reescrita: conjunto de regras    98 retorna: <isaac @ linux. org. au. >
reescrita: conjunto de regras 198entrada: <isaac @ linux. org. au. >
reescrita: conjunto de regras 95    entrada: <uucp-novo: moria> <isaac /
    @ Linux. org. au. >
reescrita: conjunto de regras 95 retorna: $ # uucp-novo $ $ @ moria:
<isaac /
    @ Linux. org. au. >
reescrita: conjunto de regras 198 retornos: $ # uucp-novo $ $ @ moria: <isaac /
    @ Linux. org. au. >
reescrita: conjunto de regras    0 devolve: $ # uucp-novo $ $ @ moria: <isaac /
    @ Linux. org. au. >
```

Os resultados deste teste indicam que o nome do host foi resolvido, e que a mensagem ainda teria sido encaminhado para o nosso host inteligente. Isso prova que o nosso `LOCAL_NET_CONFIG` definição funciona corretamente e se se tratou ambos os casos corretamente. Esse teste também foi bem-sucedido, para que possamos assumir com alegria a nossa configuração está correta e uso ele.

Correndo o sendmail

A `sendmail` daemon pode ser executado de duas formas. Uma maneira é ter que ter que correr a partir do `inetd` daemon, o alternativo, eo método mais comumente usado é para executar `sendmail` como um daemon standalone. É também comuns para os programas de mensagens para invocar `sendmail` como um comando do usuário para aceitar gerados localmente e-mail para entrega.

Ao executar `sendmail` no modo autônomo, coloque o comando em um *rc* arquivo para que ele começa na hora da inicialização. A sintaxe usada é normalmente:

```
/ Usr / sbin / sendmail-bd-q10m
```

A `-Bd` argumento diz `sendmail` para rodar como um daemon. Será garfo e executados em segundo plano. A `-Q10m` argumento diz `sendmail` verificar a sua fila a cada dez minutos. Você pode optar por usar uma fila diferente Verificação do tempo.

Para executar `sendmail` da `inetd` daemon de rede, você pode usar uma entrada como:

```
smtp  stream  tcp nowait  ninguém / Usr / sbin / sendmail-bs
```

A `-Bs` argumento aqui diz `sendmail` para utilizar o protocolo SMTP em stdin / stdout, que é necessário para o uso com `inetd`.

A `runq` comando é normalmente uma ligação simbólica para a `sendmail` binário e é uma forma mais conveniente de:

```
# sendmail-q
```

Quando `sendmail` é chamado desta forma, ele processa todo o correio de espera na fila para ser transmitido. Quando executado, ning `sendmail` a partir de `inetd` você também deve criar um `cron` trabalho que executa o `runq` comando periodicamente para garantir que o spool de email é atendido periodicamente.

Uma adequada `cron` entrada da tabela seria semelhante a:

```
# Execute o spool de email a cada quinze minutos
0,15,30,45     *     *     *     *     / Usr / bin / runq
```

Na maioria das instalações `sendmail` processos na fila a cada 15 minutos, conforme mostrado em nosso *crontab* exemplo, em-tentador para transmitir alguma mensagem lá.

Dicas e Truques

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Há uma série de coisas que você pode fazer para tornar o gerenciamento de uma `sendmail` site eficiente. Uma série de gerir-ferramentas de análise são fornecidos no `sendmail` pacote, vamos olhar para o mais importante deles.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Gerenciando o spool de email

Mail é enfileirado no */ Var / spool / mqueue* diretório antes de serem transmitidas. Este diretório é chamado o e-mail carretel. A `sendmail` programa fornece um meio de exibir uma lista formatada de todas as mensagens de correio spool e seu estatuto.

A `/ Usr / bin / mailq` comando é um link simbólico para o `sendmail` executável e se comporta indentically para:

```
# sendmail-bp
```

A saída exibe o ID da mensagem, o seu tamanho, o tempo que foi colocado na fila, que o enviou, e uma mensagem indicando seu status atual. O exemplo a seguir mostra uma mensagem de e-mail preso na fila com um problema:

```
$ mailq
                Mail Queue (um pedido)
- Q-ID - - Tamanho - ----- ----- Q-Time ------------Sender/Recipient---------- -
RAA00275      124 Qua Dez  9 17:47 raiz
                (Mapa de acolhimento: pesquisa (tao.linux.org.au): diferidos)
                                    terry@tao.linux.org.au
```

Esta mensagem ainda está na fila de e-mail porque o endereço IP do host de destino não pôde ser resolvido.

Nós podemos forçar `sendmail` para processar a fila agora, emitindo o */ Usr / bin / runq* comando.

A `runq` comando não produz saída. `sendmail` começará a processar a fila de mensagens em segundo plano.

Forçando um host remoto para o seu processo fila de correio

Se você usar uma conexão discada à Internet temporários, com um *fixo* Endereço IP e confiar em um host MX para recolher o seu
e-mail enquanto você estiver desconectado, você vai achar que é útil para forçar o host MX para processar sua fila de e-mail logo após a
você estabelecer a conexão.

Um pequeno `perl` programa está incluído com o `sendmail` distribuição que faz com que esta simples para os anfitriões e-mail que
apoiá-lo. A `etrn` script tem o mesmo efeito em um host remoto como o `runq` comando tem na nossa cabeça. Se
nós invocamos o comando como mostrado neste exemplo:

```
# vstout.vbrew.com etrn
```

vamos forçar o host vstout.vbrew.com para processar todo o correio na fila para a nossa máquina local.

Normalmente você pode adicionar esse comando no seu PPP *ip-up* script para que ele seja executado logo após a sua rede conexão é estabelecida.

Análise Estatística Mail

`sendmail` coleta dados sobre os volumes de tráfego de email e algumas informações sobre os hosts que emitiu e-mail. Existem dois comandos disponíveis para exibir essa informação, `mailstats`E `hoststat`.

mailstats

A `mailstats` comando exibe estatísticas sobre o volume de e-mail processado por `sendmail`. O momento em cuja coleta de dados iniciou é impresso em primeiro lugar, seguido por uma tabela com uma linha para cada mailer configurado e mostrando um resumo de um total de todo o correio. Cada linha apresenta oito itens de informação:

Campo	Significado
`M`	A mala direta (protocolo de transporte) Número
`msgsfr`	O número de mensagens recebidas desde o mailer
`bytes_from`	O Kbytes de correio a partir da mala direta
`msgsto`	O número de mensagens enviadas para o mailer

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`bytes_to`	O Kbytes de e-mail enviado para o mailer

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Campo	Significado
`msgsreg`	O número de mensagens rejeitadas
`msgsdis`	O número de mensagens descartadas
`Remetente`	O nome do envelope

Uma amostra da saída do `mailstats` comando é mostrado na Exemplo de 18,5.

18,5 Exemplo: exemplo de saída do comando mailstats

```
# / Usr / sbin / mailstats
Estatísticas da Sun, 20 dez 1998 22:47:02
 M   msgsfr  bytes_from   msgsto    bytes_to  msgsdis msgsrej  Remetente
 0        0          0K       19        515K        0       0  prog
 3       33        545k        0          0K        0       0  local
 5       88        972K      139       1018K        0       0  esmtp
=============================================== ===========
 T      121       1517K      158       1533K        0       0
```

Estes dados são recolhidos, se a *StatusFile* opção está habilitada no *sendmail.cf* eo arquivo de estado existe. Normalmente você pode adicionar o seguinte ao seu *sendmail.cf* arquivo:

```
# Arquivo de status
O StatusFile = / var / log / sendmail.st
```

Para reiniciar a coleta de estatísticas, você precisa fazer as estatísticas do arquivo de comprimento zero:

```
> / Var / log / sendmail.st
```

e reinicie `sendmail`.

hoststat

A `hoststat` comando exibe informações sobre o status de hosts que `sendmail` tentou de-
mail fígado. A `hoststat` comando é equivalente a chamar `sendmail` como:
sendmail-BH

A saída apresenta cada host em uma linha própria, e para cada um o tempo decorrido desde a entrega foi tentada a ele, e recebeu a mensagem de status na época.

Exemplo de 18,6 scomos o tipo de saída que você pode esperar do `hoststat` comando. Note que a maioria dos resultados indicam entrega bem sucedida. O resultado para earthlink.net, Por outro lado, indica que a entrega foi vencida. A mensagem de status às vezes podem ajudar a determinar a causa da falha. Neste caso, o cone-
ção expirou, provavelmente porque o anfitrião foi para baixo ou inacessível no tempo de entrega foi tentada.

18,6 Exemplo: exemplo de saída do comando oststat

```
# hoststat
 ---------- -------------- Hostname Como há muito tempo --------- --------- Resultados
 mail.telstra.com.au                  04:05:41 Mensagem 250 aceito para
 scooter.eye-net.com.au              81 +08:32:42 250 id = OK 0zTGai-0008S9-0
 yarrina.connect.com.a               53 +10:46:03 250 LAA09163 Mensagem acce
 happy.optus.com.au                  55 +03:34:40 250 Mail aceite
 mail.zip.com.au                      04:05:33 250 RAA23904 Mensagem acce
 kwanon.research.canon.com.au        44 +04:39:10 250 ok 911542267 qp 21186
 linux.org.au                        83 +10:04:11 250 IAA31139 Mensagem acce
 albert.aapra.org.au                  00:00:12 250 VAA21968 Mensagem acce
 field.medicine.adelaide.edu.au      53 +10:46:03 250 ok 910742814 qp 721
 copper.fuller.net                   65 +12:38:00 250 OAA14470 Mensagem acce
 amsat.org                            5 +06:49:21 250 UAA07526 Mensagem acce
 mail.acm.org                        53 +10:46:17 250 TAA25012 Mensagem acce
 extmail.bigpond.com                 11 +04:06:20 250 ok
 earthlink.net                       45 +05:41:09 diferidos: tempo de conexão
```

A `purgestat` comando libera os dados coletados de acolhimento e é equivalente a invocar o sendmail como:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# sendmail-BH
```

As estatísticas continuarão a crescer até eliminá-los. Você pode querer executar periodicamente o `purgestat` comando para facilitar a busca e encontrar as entradas mais recentes, especialmente se você tiver um local ocupado. Você poderia colocar o
comando em uma *crontab* arquivo para executá-lo automaticamente, ou simplesmente fazê-lo sozinho, ocasionalmente.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 19 - Getting Up and Running Exim

Este capítulo apresenta uma rápida introdução à criação de Exim e uma visão geral de sua funcionalidade.

Embora
Exim é amplamente compatível com `sendmail` em seu comportamento, seus arquivos de configuração são completamente diferentes.

O principal arquivo de configuração é geralmente chamada */ Etc / exim.conf* ou */ Etc / exim / config* na maioria das distribuições

Linux, ou
/ Usr / exim / lib / config em configurações mais velhos. Você pode descobrir onde o arquivo de configuração está executando o comando:

```
$ configure_file exim-bp
```

Você pode ter que editar o arquivo de configuração para refletir os valores específicos para o seu site. Na maioria das

configurações comuns
não há muito a mudar, e uma configuração de trabalho raramente terá que ser modificada.

Por padrão, o Exim processos e fornece todos os e-mails recebidos imediatamente. Se você tiver um tráfego relativamente alto,

você
pode sim ter Exim recolher todas as mensagens da chamada *fila*, E processá-los em intervalos regulares só.

Quando o tratamento do correio dentro de uma rede TCP / IP, o Exim é frequentemente executado em modo daemon: em tempo

de inicialização do sistema, é
invocados a partir de */ Etc / init.d / exim*[113] e se coloca em segundo plano, onde aguarda por conexões TCP na porta SMTP (normalmente a porta 25). Isso é benéfico, sempre que você espera ter uma quantidade significativa de Traf- Exim fic porque não tem o arranque para cada conexão de entrada. Como alternativa, `inetd` conseguissem a porta SMTP e tê-lo spawn Exim sempre que houver uma conexão nessa porta. Essa configuração pode ser útil quando você tem memória limitada e baixo volume de tráfego de correio.

Exim tem um conjunto complexo de opções de linha de comando, incluindo muitos que correspondem aos do sendmail. Em vez

de
tentando montar exatamente as opções certas para as suas necessidades, você pode implementar os tipos mais comuns de operação, invocando os comandos tradicionais, como `rmail` ou `rsmtp`. Estes são links simbólicos para Exim (ou se eles não são, você pode facilmente ligam a ele). Quando você executar um dos comandos, Exim verifica o nome usado invocá-lo e define as opções de si próprio.

Há dois links para Exim que você deve ter em todas as circunstâncias: `/ Usr / bin / rmail` e `/ Usr / sbin / sendmail`.[114] Quando você compor e enviar uma mensagem de email com um agente como `olmo`, O mes-
Sábio é canalizada para `sendmail` ou `rmail` para a entrega, razão pela qual ambos `/ Usr / sbin / sendmail` e `/ Usr / bin / rmail` deve apontar para Exim. A lista de destinatários para a mensagem é passada para Exim na com- linha de mando.[115] O mesmo acontece com o e-mail proveniente de via UUCP. Você pode configurar os caminhos necessários para apontar
para o Exim, digitando o seguinte em um prompt do shell:

```
$ ln-s / usr / sbin / exim / usr / bin / rmail
$ ln-s / usr / sbin / exim / usr / sbin / sendmail
```

Se você quiser ir mais longe nos detalhes de configuração do Exim, você deve consultar a especificação completa do Exim. Se isso não está incluído na sua distribuição Linux favorita, você pode obtê-lo desde a nascente até Exim, ou lê-lo on-line a partir do site Exim na Web em http://www.exim.org/.

Correndo Exim

Para executar o Exim, você deve primeiro decidir se você quer que lidar com mensagens de entrada SMTP funcionando como

um
daemon separado, ou se ter `inetd` gerenciar a porta SMTP e invocar Exim apenas quando um SMTP conexão é solicitada a partir de um cliente. Normalmente, você irá preferir operação daemon no servidor de correio porque

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

carrega a máquina muito menos do que a desova Exim repetidas vezes para cada ligação. Como o servidor de email também entrega de correio de entrada mais diretamente aos usuários, você deve escolher `inetd` operação na maioria dos outros hosts.

Seja qual for o modo de operação que você escolhe para cada máquina individual, você tem que fazer se você tem o seguinte entrada no seu */ Etc / services* arquivo:

113 Outras localizações possíveis são */ Etc / rc.d / init.d* e *rc.inet2*. Esta última é comum em sistemas que utilizam uma estrutura no estilo BSD para admini sistema
arquivos de demonstração no */ Etc* diretório.

114 Este é o novo local padrão de `sendmail` de acordo com o Linux File System Standard. Outro local comum é */ Usr / lib / sendmail*, Que é susceptível de ser utilizado por programas de correio que não são especialmente configurados para Linux. Você pode definir os nomes
como links simbólicos para Exim, para que programas e scripts invocando *sendmail* em vez disso, invoca o Exim para fazer as mesmas coisas.

115 Alguns agentes do usuário, no entanto, usar o protocolo SMTP para transmitir mensagens para o agente de transporte, chamando-a com o *-Bs* opção.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
smtp            25/tcp          # Simple Mail Transfer Protocol
```

Isso define o número da porta TCP que é usada para conversas SMTP. O número de porta 25 é o padrão definido pelo "Assigned Numbers" RFC (RFC-1700).

Quando executado no modo daemon, Exim se coloca no fundo e aguarda conexões na porta SMTP.
Quando a conexão ocorre, garfos, eo processo filho conduz uma conversação SMTP com o processo de peer no host chamada. O daemon do Exim é normalmente iniciado, invocando-o da *rc* script em tempo de inicialização usando o o seguinte comando:

```
/ Usr / sbin / exim-q15m-bd
```

A *-Bd* flag ativa o modo daemon, e *-Q15m* torna qualquer processo de mensagens se acumularam na fila de mensagens a cada 15 minutos.

Se você quiser usar `inetd` em vez disso, seu */ Etc / inetd.conf* arquivo deve conter uma linha como esta:

```
smtp    stream  tcp nowait  root  / Usr / sbin / exim   in.exim-bs
```

Lembre-se que você tem que fazer `inetd` re-leitura *inetd.conf* , enviando-lhe uma *HUP* sinal depois de fazer qualquer alterações.[116]

Daemon e `inetd` modos são mutuamente exclusivos. Se você executar Exim em modo daemon, você deve certificar-se comente qualquer linha em *inetd.conf* para o *smtp* serviços. Equivalentemente, ao ter `inetd` gerenciar Exim, fazer certeza de que não *rc* script inicia o daemon do Exim.

Você pode verificar que o Exim está corretamente configurado para receber mensagens de SMTP por telnet para o SMTP porta em sua máquina. Isto é o que o sucesso se conectar ao servidor SMTP aparência:

```
$ smtp telnet localhost
Trying 127.0.0.1 ...
Connected to localhost.
Escape character is'^]'.
220 richard.vbrew.com ESMTP Exim 3,13 # 1 Sun, 30 de janeiro de 2000 16:23:55 0600
parar
221 Fechando conexão richard.brew.com
Ligação fechada pelo anfitrião estrangeiro.
```

Se este teste não produzir o banner SMTP (a linha de partida com o código 220), verifique se você quer executar-se ning um processo daemon do Exim ou ter `inetd` configurado corretamente. Se isso não revelar o problema, procure na os arquivos de log do Exim (descrito a seguir), caso haja um erro no arquivo de configuração do Exim.

Se seu e-mail por não conseguir

Uma série de recursos estão disponíveis para solucionar problemas de instalação. O primeiro lugar a checar é Exim arquivos de log. Em sistemas Linux são normalmente mantidas em */ Var / log / exim / log* e são nomeados *exim_mainlog*, *exim_rejectlog*E *exim_paniclog*. Em outros sistemas operacionais, são frequentemente mantidos em */ Var / spool / exim / log*. Você pode descobrir onde os arquivos de log estão executando o comando:

```
log_file_path exim-bp
```

O registro de todas as principais listas de operações, a rejeição de log contém detalhes das mensagens que foram rejeitados por razões políticas
filhos, eo log de pânico é para mensagens relacionadas a erros de configuração e assim por diante.

Entradas típicas no log principal são mostradas abaixo. Cada entrada no log em si é uma única linha de texto, começando com uma data e hora. Eles foram divididos em várias linhas aqui, a fim de encaixá-los na página:

```
2000/01/30 15:46:37 12EwYe-0004WO-00 <jack@vstout.vbrew.com =
  Vstout.vbrew.com H = [192.168.131.111] U = P = ESMTP Exim S = 32100
  id = 38690D72.286F vstout.vbrew.com @
2000/01/30 15:46:37 12EwYe-0004WO-00 = <jill@vbrew.com> jill>
  D = T = localuser local_delivery
2000/01/30 15:46:37 12EwYe-0004WO-00 Terminado
```

---

[116] Use `matar HUP` *pid*, para os quais *pid* é a identificação do processo do `inetd` recuperado de um processo `ps` anúncio.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Essas entradas mostram que uma mensagem de jack@vstout.vbrew.com para jill@vbrew.com foi entregue com êxito uma caixa de correio na máquina local. chegadas Mensagem são sinalizadas com <=, E as entregas com =>.

Existem dois tipos de erros de entrega: permanentes e temporários. Um erro de entrega permanente é registrada em um log entrada como esta, marcada com "**":

```
2000/01/30 14:48:28 12EvcH-0003rC-00 bill@lager.vbrew.com **
  R = T = lookuphost smtp: SMTP erro de mailer remoto após RCPT TO:
  <bill@lager.vbrew.com>: lager.vbrew.com host [192.168.157.2]:
  550 <bill@lager.vbrew.com> ... Usuário desconhecido
```

Após uma falha como essa, Exim envia um relatório de falha na entrega, muitas vezes chamado de *mensagem de retorno* de volta para o remetente.

erros temporários são sinalizados com "==":

```
2000/01/30 12:50:50 12E9Un-0004Wq-00 jim@bitter.vbrew.com ==
  T = smtp adiar (145): Connection timed out
```

Este erro é típico de uma situação em que o Exim corretamente reconhece que a mensagem deve ser entregue a um host remoto, mas não é capaz de se conectar ao serviço SMTP em que o anfitrião. O hospedeiro pode ser baixo ou não pôde ser um problema de rede. Sempre que uma mensagem é *diferidos* assim, ele permanece na fila do Exim e é repetida na intervals. No entanto, se não conseguir ser entregue por um tempo suficientemente longo (geralmente vários dias), um erro permanente ocorre ea mensagem é devolvida.

Se você não conseguir localizar o problema da mensagem de erro Exim gera, você pode querer ligar de-escuta as mensagens. Você pode fazer isso usando o *-D* bandeira, opcionalmente seguido por um número que especifica o nível de verbosidade (um valor de 9 dá o máximo de informação). Exim, em seguida, exibe um relatório de sua operação na tela, que pode lhe dar mais dicas sobre o que está acontecendo de errado.

Compilando Exim

Exim ainda está em desenvolvimento ativo; a versão do Exim incluído nas distribuições Linux não é provavelmente a versão mais recente. Se você precisa de um recurso ou uma correção de bug encontrado em uma versão posterior, você tem que obter uma cópia da fonte código e compilá-la. A última versão pode ser encontrada através da página na web do Exim http://www.exim.org/.

Linux é um dos muitos sistemas operacionais suportados pela fonte Exim. Para compilar o exim para Linux, você deve editar o *src / EDITME* arquivo e colocar o resultado em um arquivo chamado *Local / Makefile*. Há comentários na *src / EDITME* que lhe dizem que as várias definições são utilizadas. Em seguida, execute `fazer`. Consulte o manual do Exim para de-mações sobre Exim construção da fonte.

Modos de entrega de correio

Como observado anteriormente, o Exim é capaz de entregar mensagens imediatamente ou fila-los para posterior processamento.

Todos os em-e-mail proveniente está armazenado no *Entrada* diretório abaixo */ Var / spool / exim*. Quando a fila não estiver em operação, uma entrega processo é iniciado para cada mensagem assim que ela chega. Caso contrário, ele fica na fila até que um *fila-runner* processo de pega. Filas podem ser feitas através da criação incondicional *queue_only* no arquivo de configuração, ou pode sujeita à carga do sistema de 1 minuto por uma configuração, tais como:

```
queue_only_load = 4
```

que faz com que as mensagens sejam enfileiradas, se a carga do sistema for superior a 4.[117]

Se o host não estiver permanentemente conectado à Internet, você pode querer ligar à espera dos anúncios remoto vestidos, permitindo Exim para realizar partos local imediatamente. Você pode fazer isso através da criação:

```
queue_remote_domains = *
```

no arquivo de configuração.

Se você ligar de qualquer forma de filas, você tem que certificar-se as filas são verificadas regularmente, provavelmente a cada

PDF Creator - PDF 4 free v2.0 http://www.pdf4free.com

ou 15 minutos. Mesmo sem nenhuma opção explícita de filas, as filas devem ser verificados para as mensagens que foram adiadas por causa de falhas na entrega temporária. Se você executar Exim em modo daemon, você deve adicionar o -

117 A carga do sistema é uma medida padrão do Unix da média do número de processos que estão na fila, esperando para ser executado. A `uptime` mostra as médias de carga tomadas nos últimos 1, 5 e 15 minutos.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

q15m opção na linha de comando para processar a fila a cada 15 minutos. Você também pode invocar `exim-q` a partir de `cron` nesses intervalos.

Você pode visualizar a fila de email atual, invocando com o Exim *Pb* opção. Equivalentemente, você pode fazer `mailq` um link para o Exim, e invocar `mailq`:

```
$ mailq
 2h    52K 12EwGE-0005jD-00 <sam@vbrew.com>
         bob@vbrew.com D
           harry@example.net
```

Isso mostra uma única mensagem de sam@vbrew.com a dois destinatários sentado na fila de mensagens. Ele foi entregue ao bob@vbrew.com, mas ainda não foi entregue ao harry@example.net, embora tenha estiveram na fila por duas horas. O tamanho da mensagem é 52K, ea identificação de Exim, que identifica este mes-sábio é `12EwGE-0005jD-00`. Você pode descobrir por que a entrega ainda não está completo, observando a mes-arquivo de log individuais sábio, que é mantido na *msglog* diretório diretório de spool do Exim. A *-MVL* opção é uma maneira fácil de fazer isso:

```
$ exim-MVL 12EwGE-0005jD-00
2000/01/30 example.net 17:28:13 [192.168.8.2]: Connection timed out
2000/01/30 17:28:13 harry@example.net: transporte remote_smtp diferido:
  A conexão expirou
```

arquivos de log individuais de manter uma cópia de entradas de log para cada mensagem que você possa facilmente inspecioná-los. As mesmas informações
informações poderiam ter sido extraídos do arquivo de log principal utilizando o `exigrep` utilidade:

```
$ exigrep 12EwGE-0005jD-00 / var / log / exim / exim_mainlog
```

Isso levaria mais tempo, especialmente em um sistema ocupado, onde os arquivos de log pode ficar muito grande. A `exigrep` utilitário entrar em seu próprio, ao procurar informações sobre mais de uma mensagem. Seu primeiro argumento é um regular expressão, e ele pega todas as linhas de log preocupados com as mensagens que têm pelo menos uma linha de log que corresponde à expressão. Assim, ele pode ser usado para escolher todas as mensagens para um endereço específico, ou todos aqueles ou
a partir de um determinado host.

Você pode manter uma vigilância geral sobre o que é um Exim rodando faz por execução `cauda` em seu arquivo de log principal. Outro
maneira de fazer isso é executar o `eximon` utilitário que vem com o Exim. Este é um aplicativo X11 que coloca uma exibição de rolagem do registro principal, e também mostra uma lista de mensagens que estão aguardando a entrega, bem como algumas
stripcharts sobre a atividade de entrega.

Diversas opções de configuração

Aqui estão algumas das opções mais úteis que você pode definir no arquivo de configuração:

message_size_limit

Definir esta opção limita o tamanho da mensagem que o Exim irá aceitar.

return_size_limit

Definir essa opção limita a quantidade de uma mensagem recebida que Exim retornará como parte de uma mensagem de rejeição.

deliver_load_max

Se a carga do sistema ultrapassa o valor dado para esta opção, todas as entregas de correio está suspenso, mas as mensagens são continuam a ser aceites.

smtp_accept_max

Este é o número máximo de chamadas simultâneas SMTP Exim está disposta a aceitar.

log_level

Esta opção controla a quantidade de material que está escrito no log. Existem também algumas opções de nomes começando com *log_* que controlam o registro de informações específicas.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Mensagem de roteamento e entrega

Exim divide-se a entrega de correio em três tarefas diferentes: encaminhamento, orientação e transporte. Há uma série de módulos de código de cada tipo, e cada um é separadamente configurável. Normalmente, uma série de roteadores diferentes, diretores,
e transportes são configurados no arquivo de configuração.

Roteadores resolver endereços remotos, determinando que acolhem a mensagem deve ser enviada e que o transporte deve ser usado. Em hosts conectados à Internet muitas vezes há apenas um roteador, que faz a resolução, observando o domínio no DNS. Alternativamente, pode haver um roteador que manipula os endereços destinados a hosts em um Rede local, e um segundo para enviar quaisquer outros endereços para um único *host inteligente*, Por exemplo, um servidor de correio do ISP.

Local endereços são dadas aos diretores, dos quais normalmente há vários, para lidar com aliasing e encaminhamento
bem como identificar as caixas de correio local. As listas de discussão podem ser tratadas por diretores aliasing ou encaminhar. Se um
endereço é alias ou encaminhados, os endereços gerados são tratados de forma independente pelos roteadores ou diretores,
conforme necessário. De longe, o caso mais comum será a entrega de uma caixa de correio, mas as mensagens também pode ser canalizada para uma
comando ou anexado a um arquivo diferente na caixa de correio padrão.

Um transporte é responsável por implementar um método de entrega, por exemplo, enviando a mensagem através de uma SMTP conexão ou adicioná-la a uma caixa postal específica. Roteadores e diretores selecionar qual o transporte a utilizar para cada
endereço do destinatário. Se o transporte falha, Exim ou gera uma mensagem de rejeição ou adia o endereço para uma posterior repetição.

Com Exim, você tem muita liberdade de configuração dessas tarefas. Para cada um deles, um número de condutores estão disponível, a partir do qual você pode escolher aqueles que você precisa. Descrevê-los para o Exim em diferentes seções da sua arquivo de configuração. Os transportes são definidos em primeiro lugar, seguidos pelos administradores e, em seguida os roteadores. Não há
built-in padrão, embora Exim é distribuído com um arquivo de configuração padrão, que inclui os casos simples. Se você quero mudar a política de roteamento Exim ou modificar um transporte, é mais fácil iniciar a partir da configuração padrão e fazer mudanças em vez de tentar definir uma configuração completa do zero.

Roteamento de mensagens

Quando um determinado endereço de entrega, Exim verifica primeiro se o domínio é aquele que é tratado no host local combinando isso com uma lista na `local_domains` configuração variável. Se essa opção não for definida, o local nome do host é usado como o único domínio local. Se o domínio for local, o endereço é entregue aos administradores. Outros-sábio, ela é entregue aos roteadores para descobrir qual host de transmitir uma mensagem.[118]

Entrega de mensagens para endereços locais

Mais comumente, um endereço local é apenas um nome de login do usuário, caso em que a mensagem é entregue ao usuário caixa de correio, */ Var / spool / mail/nome de usuário*. Outros casos incluem pseudónimos, nomes de lista de discussão e encaminhamento de mensagens pela
usuário. Nestes casos, o endereço do local se expande para uma nova lista de endereços, que pode ser local ou remoto.

Para além destas "normal" endereços, Exim pode lidar com outros tipos de mensagem destinos locais, como nomes de arquivos e os comandos da tubulação. Ao entregar a um arquivo, Exim acrescenta a mensagem, criar o arquivo se necessário. Arquivo e Destinos tubo não são endereços por direito próprio, então você não pode enviar email para, digamos, / etc / passwd vbrew.com @
e esperar para substituir o arquivo de senhas; entregas para um arquivo específico são válidos apenas se forem provenientes de transmitir-
ção ou arquivos de alias. Observe, entretanto, que o / etc / passwd vbrew.com @ é um endereço de e-mail sintaticamente válido, mas se Exim
recebido, que seria (tipicamente) de pesquisa para um usuário cujo nome de login foi / etc / passwd, não conseguem encontrar um lado, ea rejeição
a mensagem.

Em uma lista ou um arquivo de encaminhamento alias, um *nome do arquivo* é qualquer coisa que começa com uma barra (/) que não analisa como um sistema de

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

e-mail qualificado. Por exemplo, */ Tmp / lixo* na transmissão ou arquivo de alias é interpretado como um nome de arquivo, mas / Lixo / tmp vbrew.com @ é um endereço de e-mail, embora não seja susceptível de ser muito útil. No entanto, ad-válidos vestidos deste tipo são vistos ao enviar e-mail através de gateways X.400, porque os endereços X.400 começar com uma barra.

118 Esta é uma simplificação. É possível para os diretores de passar os endereços para os transportes com entrega em máquinas remotas, e da mesma forma, é possível

para roteadores para transmitir endereços de locais que transporta a mensagem para a gravação de um arquivo ou um cachimbo. Também é possível para os roteadores para transmitir endereços
aos diretores, em algumas circunstâncias.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Da mesma forma, um *comando pipe* pode ser qualquer comando do Unix precedidas pelo símbolo pipe (|), a menos que analisa a cadeia
como um endereço válido de email com domínio completo. A menos que tenha mudado a configuração, o Exim não usa um shell para executar o comando, em vez disso, ele divide-o em um nome de comando, os argumentos em si, e executa-lo diretamente. A
mensagem é alimentado para o comando em sua entrada padrão.

Por exemplo, a porta de uma lista de discussão em um grupo de notícias local, você pode usar um script shell chamado

`gateit`E defina
um alias local que oferece todas as mensagens de mailing list para o script usando `| Gateit`. Se o comando
linha contém uma vírgula, e que o símbolo pipe anterior deve ser colocado entre aspas duplas.

Os usuários locais

Um endereço de locais mais comumente denota uma caixa de correio do usuário. Isto é normalmente localizado em */ Var / spool / mail* e tem a
nome do usuário, que também é dono do arquivo. Se ele não existir, é criado por Exim.

Em algumas configurações, o grupo está definido para o grupo do usuário eo modo é 0600. Nestes casos, proc-entrega cessos são executados como o usuário, eo usuário pode excluir totalmente a caixa de correio. Em outras, a caixa de correio grupo é *e-mail*, E tem modo 660; processos de entrega são executados sob um sistema de uid e de grupo *e-mail*, E os usuários não pode apagar seus arquivos de caixa de correio, embora eles possam esvaziá-las.

Observe que, embora */ Var / spool / mail* é actualmente o local padrão para colocar os arquivos caixa de entrada, alguns

softwares de email
pode ser compilado para usar caminhos diferentes, por exemplo, */ Usr / spool / mail*. Se a entrega para os usuários em sua máquina não
consistentemente, você deve ver se isso ajuda a fazer deste um link simbólico para */ Var / spool / mail*.

Os endereços *MAILER DAEMON-* e *postmaster* deve aparecer normalmente em seu arquivo de alias, expandindo para o endereço de email do administrador do sistema. *MAILER DAEMON-* é usado pelo Exim como o endereço do remetente no salto mensagens. Também é recomendado que *root* ser configurado como um apelido para um administrador, especialmente quando as entregas
estão sendo executados com as permissões dos usuários do destinatário, para evitar correr qualquer tipo de parto como *root*.

Encaminhamento

Os usuários podem redirecionar suas mensagens para os endereços alternativos, criando uma *. Avançar* arquivo em seus

diretórios. Este
contém uma lista de destinatários separados por vírgulas e / ou novas linhas. Todas as linhas do arquivo são lidos e interpretados. Qualquer tipo de endereço pode ser usado. Um exemplo prático de uma *. Avançar* ficheiro de férias pode ser:

```
Janet, "| férias"
```

Em outras descrições de *. Avançar* arquivos, você pode ver o nome no início precedido por uma barra invertida. Esta foi necessária em alguns MTAs mais para parar a busca de um *. Avançar* para o novo nome, que poderia levar a looping.
A barra invertida não é necessária no Exim, que automaticamente evita loops deste tipo.[119] No entanto, uma barra invertida é permitido, e de fato faz a diferença em configurações em vários domínios estão sendo tratadas no
uma vez. Sem uma barra invertida, um nome não qualificado é qualificado, com um domínio padrão, com uma barra invertida a domínio de entrada é preservada.

O primeiro endereço no arquivo de transmitir entrega a mensagem recebida para janet'Caixa de s, enquanto o `férias` comando retorna uma notificação abreviado para o remetente.[120]

Além do apoio à "tradicional" arquivos de encaminhamento, Exim pode ser configurado para permitir que arquivos mais

complexos
chamada *filtros*. Em vez de ser apenas uma lista de endereços de encaminhamento, um filtro de arquivo pode conter provas sobre o conteúdo do
a mensagem recebida para que, por exemplo, as mensagens podem ser enviadas somente se o assunto contidas no mes-sábio "urgente". O administrador do sistema deve decidir se vai permitir que os usuários dessa flexibilidade.

Alias Arquivos

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Exim é capaz de lidar com arquivos compatíveis com o apelido de Berkeley `sendmail` arquivos de alias. As entradas no

arquivo de alias pode
ter a seguinte forma:
alias`:` *destinatários*

119 Um diretor é ignorada se o endereço está prestes a processo é que previamente tratados no curso de gerar o presente
endereço.
120 Por favor, se você optar por usar um programa de férias, certifique-se que não vai responder a mensagens enviadas a partir de listas de discussão! É muito chato
descobrir que alguém tenha ido de férias e encontrar uma mensagem de férias para cada mensagem que tenho recebido. lista de administradores para correspondência:
este é um bom exemplo de porque é uma má prática para forçar o `Responder para:` campo de mensagens da lista de discussão para que a apresentação da lista
endereço.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

destinatários é uma lista separada por vírgula de endereços que serão substituídos para o alias. A lista de destinatários pode ser continuada através newlines se a linha seguinte começa com um espaço.

Uma característica especial permite Exim para manipular as listas de discussão que são mantidos separadamente do arquivo de alias: se você especificar `: Incluem:`*nome do arquivo* como destinatário, o Exim lê o arquivo especificado e substitui o seu conteúdo como uma lista de destinentos. Uma alternativa para o tratamento de listas de discussão é mostrado mais adiante neste capítulo em "Listas de Discussão".

O arquivo de aliases principal é */ Etc / aliases*. Se você fizer este arquivo graváveis gravável ou em grupo, Exim irá se recusar a usá-lo e adiar entregas locais. Você pode controlar o teste se aplica para as permissões do arquivo de configuração *de modo máscara* na *system_aliases* diretor.

Esta é uma amostra *aliases* arquivo:

```
# Vbrew.com arquivo / etc / aliases
hostmaster: janet
postmaster: janet
usenet: phil
# A lista de discussão do desenvolvimento.
desenvolvimento: a marca de joe, processar, biff,
        / Var / mail / log / desenvolvimento
desenvolvimento proprietário: joe
# Avisos de interesse geral, são enviados a todos os
# Do pessoal
anunciar:: include: / etc / exim / pessoal,
        / Var / mail / log / anunciar
proprietário anunciar: root
# Porta a lista de discussão de PPP para um grupo de notícias local
lista PPP: "| / usr / local / bin / local.lists.ppp gateit"
```

Quando há nomes de arquivos e comandos tubulação em um arquivo de alias, como aqui, Exim precisa ser informado que userid para executar as entregas ao abrigo. A *usuário* opção (e possivelmente *grupo*, Também) deve ser definido no arquivo de configuração do Exim, quer por o diretor que está a lidar com os apelidos, ou no transporte a que se dirige a esses itens.

Se ocorrer um erro ao entregar a um endereço gerado a partir do *aliases* arquivo, o Exim irá enviar um mes-bounce sábio ao remetente da mensagem, como de costume, mas isso pode não ser adequado. A *errors_to* opção pode ser usada para especificar que as mensagens de retorno devem ser enviadas em outros lugares, por exemplo, para o postmaster.

Listas de Discussão

Em vez do *aliases* , listas de discussão também podem ser gerenciados por meio um *forwardfile* diretor. As listas são todos mantidos em um único diretório, tais como */ Exim / etc / listas /*, E uma lista de discussão chamada *nag-bugs* é descrito pelo arquivo */ listas / nag-bugs*. Este deve conter os endereços dos membros separados por vírgulas ou novas linhas. Linhas de início com uma cerquilha (#) São tratadas como comentários. Um diretor simples de usar tais dados é a seguinte:

```
listas:
  driver = forwardfile
  file = / exim / etc / lists / $ {} local_part
  no_check_local_user
  errors_to = $ {} local_part solicitação
```

Quando esse diretor é executado, os valores dos *arquivo* e *errors_to* opções são *expandida*. Expansão certas causas parcelas das cadeias que começam com caracteres dólar ser substituído a cada tempo que a string é usada. O mais simples tipo de expansão é a inserção do valor de uma das variáveis do Exim, e é isso que está acontecendo aqui. A substring `$ {} Local_part` substitui o valor do `$ Local_part`, Que é a parte local do endereço que está sendo processado.

Para cada lista, um usuário (ou alias ou lista de discussão) chamado */istname-request* Deve existir, qualquer ocorrência de erros ao resolver um endereço ou entrega a um membro da lista são relatados para este endereço.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Proteção contra Spam Mail

*Spam Mail*Ou publicidade de e-mail não solicitadas, é um problema irritante para muitos usuários. Um projeto foi formado para resolver este problema chamado Mail Abuse Protection System (MAPS), e um mecanismo que foi construído reduz o problema, chamado de Tempo Real Blackhole List (RBL). Informações sobre como funciona o MAPS RBL pode ser obtido a partir de sua documentação on-line em http://maps.vix.com/rbl/.A idéia é simples. Sites que são capturados geração de spam e-mail são adicionadas ao banco de dados e agentes de transferência de email como o Exim é capaz de consultar o
banco de dados para confirmar que a fonte não é um spammer antes de aceitá-mail dele.

Desde o advento da RBL, várias outras listas semelhantes foram criados. Uma das mais úteis é o dial-up List (DUL), que lista os endereços IP dos hosts dial-up. Estes devem normalmente enviar mails só para os seus ISP servidores de correio. Muitos sites de e-mail bloco de externo dial-up, porque quando um host tal, evita o seu próprio provedor de
servidor, geralmente é até bom.

Exim oferece suporte para o tempo real e outras listas negras. É muito fácil configuração. Para ativá-lo, adicione o seguintes linhas ao seu */ Etc / exim.conf* arquivo:

```
# Vixie / MAPS RBL (http://maps.vix.com/rbl)
rbl_domains rbl.maps.vix.com =: dul.maps.vix.com
```

Este exemplo verifica tanto os RBL eo DUL, rejeitando todas as mensagens de hosts que estão em qualquer lista. A *rbl_hosts* opção permite que você especifique os grupos de hosts para os quais a verificação RBL faz (ou não) se aplicam. A configuração padrão é:

```
rbl_hosts = *
```

o que significa que todos os hosts estão sujeitos a verificação de RBL. Se você quisesse substituir na lista negra e aceitar e-mail a partir de um determinado host sem realizar a verificação RBL você poderia, por exemplo, use:

```
rbl_hosts =! nocheck.example.com: *
```

O ponto de exclamação antes do primeiro item desta lista indica um item negada: se o host é chamado no-check.example.com, vai corresponder a esse item. Mas por causa da negação, verificando RBL não é realizada. Qualquer outro host coincide com o segundo item na lista.

Instalação UUCP

Exim não possui código específico para o transporte de mensagens via UUCP, nem suportar UUCP caminho bang endereços. No entanto, se tratar de domínio está sendo utilizado, Exim pode ser conectado ao UUCP bastante simples. Aqui está um fragmento de configuração para o envio de determinados domínios ao UUCP, provenientes de uma instalação real:

```
# Transportes
uucp:
  tubo de motorista =
  ninguém user =
  comando = "/ usr / local / bin / uux-r - \
    $ {Substr_-5: $ host} {$ rmail local_part} "!
  return_fail_output = true

# Roteador
uucphost:
  transporte = uucp
  domainlist driver =
  route_file = / usr / exim / uucphosts
  lsearch search_type =
```

Em um arquivo de configuração completa, o transporte deve ser inserido entre os outros transportes, eo roteador provavelmente, definido como o primeiro roteador. O arquivo */ Usr / exim / uucphosts* contém entradas como esta:

```
darksite.example.com:           darksite.UUCP
```

que é interpretada para significar "Enviar e-mail endereçado ao domínio darksite.example.com para o host UUCP darksite. "Esta configuração pode ser configurado de forma mais simples sem o roteador adicionando o sufixo. UUCP para escuro
site só para ter o transporte de tirá-lo novamente, mas desta forma é útil porque torna clara a distinção ser-entre o nome de domínio darksite.example.com eo nome do host UUCP darksite.

Sempre que o router vem através de um domínio que está no arquivo de rota, ele irá enviar o endereço para o UUCP trans-porto, que, posteriormente, tubos para o uux comando (descrito no Capítulo 16, *Gerenciando UUCP Taylor*). Se

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

existe um problema, `uux` vai gerar alguma saída e terminar com um código de erro diferente de zero. A fixação de `return_fail_output` garante que a saída é devolvida ao remetente.

Se as mensagens recebidas UUCP são agrupados em arquivos no formato SMTP lote, podem ser passadas diretamente para o Exim usando um comando como este:

```
exim-bs </ var/uucp/incoming/001
```

No entanto, existe uma captura. Quando Exim recebe uma mensagem localmente, ele insiste em que o remetente é o registrado em
usuário que o chama, mas para um lote UUCP queremos que os remetentes a serem tomadas a partir das mensagens recebidas. Exim irá
fazer isso se o processo que chama é executado como um *confiança do usuário*. Se você mandar para o UUCP de entrada para ser tratado
por um usuário chamado *uucp*, Por exemplo, é necessário especificar:

```
trusted_users = uucp
```

no arquivo de configuração do Exim para garantir que os endereços do remetente é tratado corretamente.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 20 - Netnews

Netnews ou notícias Usenet, continua sendo um dos serviços mais importantes e valorizadas em redes de computadores hoje. Demitido por alguns como um lodo de e-mails comerciais não solicitados e pornografia, Netnews ainda mantém vários casos de grupos de discussão de alta qualidade que a tornou um recurso crítico em dias pré-web. Mesmo nestes vezes de um bilhão de páginas da web, Netnews ainda é uma fonte de ajuda on-line e da comunidade em muitos tópicos.

História da Usenet

A idéia da rede de notícias nasceu em 1979, quando dois estudantes de pós-graduação, Tom Truscott e Jim Ellis, o pensamento

de
usando UUCP para se conectar máquinas de troca de informações entre os usuários de Unix. Eles montaram uma pequena rede de
três máquinas na Carolina do Norte.

Inicialmente, o tráfego foi tratada por um conjunto de scripts shell (posteriormente reescrito em C), mas eles nunca foram

liberados para
o público. Eles foram rapidamente substituídos por "A Notícia", a primeira versão pública do software da notícia.

A notícia não foi projetado para lidar com mais de alguns artigos, por grupo e dia. Quando o volume continuou a crescer, ele foi reescrito por Mark Horton e Matt Glickman, que chamou o lançamento de "B" (aka B News). A primeira versão pública de B News foi a versão 2.1 em 1982. Foi ampliado de forma contínua, com várias novas funcionalidades acrescentou. Sua versão atual é B News 2.11. Ele está lentamente se tornando obsoleto; seu mantenedor oficial última mudado para
DCI.

Geoff Collyer e Henry Spencer reescreveu B News e lançado em 1987, este é o lançamento de "C", ou C News. Desde seu lançamento, tem havido uma série de patches para C News, o mais importante, a C notícias de Desempenho Release. Em sites que carregam um grande número de grupos, a sobrecarga envolvida na frequência invocando `re-laynews`, Que é responsável por despachar os artigos de entrada para outras máquinas, é significativa. O desempenho Versão adiciona uma opção para `relaynews` que permite que ele seja executado em *modo daemon*, Através do qual o programa coloca
se no fundo. O desempenho é o lançamento versão C News, actualmente incluídos na maioria dos re-Linux arrendamentos. Nós descrevemos C notícias em detalhe no Capítulo 21, *C News*.

Todos os releases até C foram direcionados principalmente para as redes UUCP, embora possam ser utilizados em outras ambientes, como bem. Eficiente de transferência de notícias através de redes como TCP / IP ou DECNet necessário um novo regime. Assim
em 1986, o *Network News Transfer Protocol* (NNTP) foi introduzido. É baseado em conexões de rede e especifica uma série de comandos de forma interativa de transferência e recuperação dos artigos.

Há uma série de aplicativos baseados em NNTP disponível a partir do líquido. Um deles é o `nntpd` por pacote Brian Barber e Phil Lapsley, que você pode usar para oferecer um serviço newsreading a um número de hosts dentro de uma rede local. `nntpd` foi concebido para complementar pacotes de notícias, como B ou C News Notícias, dar-lhes NNTP recursos. Se você pretende utilizar com o servidor NNTP News C, você deve ler o Capítulo 22, *NNTP e os Daemon nntpd*, Que explica como configurar o `nntpd` "daemon" e executá-lo com C News.

Um pacote de alternativas de apoio NNTP é DCI, ou *Internet News*. Não é apenas um frontend, mas um sistema de notícias em seu próprio direito. Dispõe de um daemon relé sofisticados notícia de que pode manter vários links simultâneos NNTP eficientemente, e é, portanto, o servidor de notícias de escolha para muitos sites da Internet. Nós discutimos isso em pormenor no capítulo
23, *Internet News*.

Qual é qual, afinal?

Um dos fatos mais impressionantes sobre a Usenet é que não faz parte de nenhuma organização, nem tem qualquer tipo de autoridade de gestão centralizada da rede. Na verdade, é parte do folclore da Usenet que, exceto por uma descrição técnica, você não pode definir *o que* é, sob o risco de soar estúpido, pode-se definir a Usenet como uma colaboração de sepa-
sites de notícias de que a taxa de câmbio da Usenet. Para ser um site Usenet, tudo que você tem a fazer é encontrar um outro

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

local da Usenet e greve
um acordo com seus proprietários e mantenedores de trocar mensagens com você. Proporcionar um outro site com notícias é chamada *alimentação* ela, de onde um outro axioma comum de filosofia da Usenet origina: "Tenha um animal, e você está nele."

A unidade básica de notícias da Usenet é o *artigo*. Esta é uma mensagem de um usuário escreve e "posts" para a rede. Para permitir que os sistemas de notícias para lidar com isso, é prefixado com informações administrativas, o cabeçalho do artigo chamados.

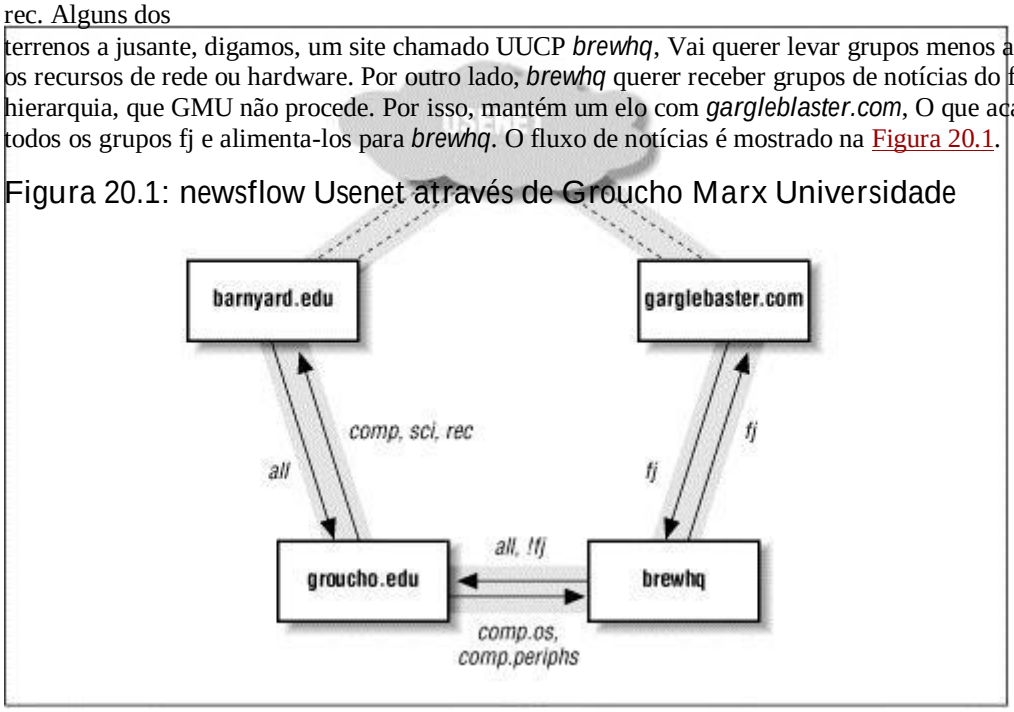
PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

É muito semelhante ao formato de cabeçalho de correio previsto no e-mail padrão Internet RFC-822, em que ela consiste de várias linhas de texto, cada um começa com um nome de domínio terminados por dois pontos, que é seguido pelo de campo valor.[121]

Os artigos são submetidos a um ou mais *newsgroup*. Pode-se considerar um grupo de discussão um fórum para artigos relativos à
um tema comum. Todos os newsgroups estão organizados em uma hierarquia, com o nome de cada grupo, indicando o seu lugar no
hierarquia. Isso muitas vezes faz com que seja fácil de ver que um grupo tem tudo a ver. Por exemplo, qualquer um pode ver a partir do
newsgroup comp.os.linux.announce nome que é usado para anúncios sobre um sistema operacional de computador
TEM chamado Linux.

Estes artigos são então trocadas entre todos os sites da Usenet que estão dispostos a levar notícias deste grupo. Quando dois locais concordam em trocar notícias, eles são livres para trocar o que eles gostam de newsgroups, e pode até mesmo adicionar
suas próprias hierarquias locais de notícias. Por exemplo, *groucho.edu* pode ter um link para notícias *barnyard.edu*, Que é um feed de notícias importantes e vários links para sites menores, que se alimenta de notícias. Agora Barnyard College pode receber todos os
grupos da Usenet, enquanto GMU só quer levar um pequeno número de grandes hierarquias, como ficção científica, comp, ou rec. Alguns dos
terrenos a jusante, digamos, um site chamado UUCP *brewhq*, Vai querer levar grupos menos ainda, porque eles não têm os recursos de rede ou hardware. Por outro lado, *brewhq* querer receber grupos de notícias do fj
hierarquia, que GMU não procede. Por isso, mantém um elo com *gargleblaster.com*, O que acarreta
todos os grupos fj e alimenta-los para *brewhq*. O fluxo de notícias é mostrado na Figura 20.1.

Figura 20.1: newsflow Usenet através de Groucho Marx Universidade



Os rótulos das setas oriundos *brewhq* pode exigir alguma explicação, no entanto. Por padrão, ele quer que todos os notícias geradas localmente para serem enviados para *groucho.edu*. No entanto, como *groucho.edu* não realizar os grupos fj, há nenhum ponto em enviar as mensagens dos grupos. Portanto, a alimentação de *brewhq* a GMU é rotulado `todos,! fj`, O que significa que todos os grupos, exceto os que estão abaixo fj são enviadas para ele.

Como a Usenet News punho?

Hoje, Usenet cresceu para enormes proporções. Sites que carregam toda a Netnews normalmente transferência de alguns, coisa como um reles 60 MB por dia.[122] Naturalmente, isso exige muito mais do que empurrar em torno de arquivos. Então vamos tomar uma
analisar a forma como a maioria dos sistemas Unix manipular notícias Usenet.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

121 O formato das mensagens de notícias da Usenet é especificado na RFC-1036, "Norma para troca de mensagens de USENET."
122 Espere um minuto: 60 Megs a 9.600 bps, que é 60 milhões, multiplicado por 1.024, ou seja ... murmurar, balbuciar ... Hey! Isso é 34 horas!

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Notícias começa quando os usuários criar e publicar artigos. Cada usuário digita uma mensagem em um aplicativo especial chamado
leitor, que formata-lo adequadamente para a transmissão ao servidor de notícias local. Em ambientes Unix, o
leitor utiliza geralmente a `inews` comando para transmitir artigos para o servidor de notícias usando o protocolo TCP / IP protocol. Mas também é possível escrever o artigo diretamente em um arquivo em um diretório especial chamado o spool de notícias. Uma vez
o lançamento é entregue ao servidor de notícias local, assume a responsabilidade de entregar o artigo para outras notícias usuários.

Notícias é distribuída através da rede por vários transportes. O meio utilizado para ser UUCP, mas hoje o principal
tráfego é feita por sites da Internet. O algoritmo de roteamento utilizado é chamado *inundações*. Cada site mantém um número de
links (*feeds de notícias*) Para outros sites. Qualquer artigo gerados ou recebidos pelo sistema de notícias local é encaminhado para
eles, a não ser que já tenha sido naquele local, caso em que ela é descartada. Um site pode encontrar informações sobre todos os outros sites
o artigo já percorrido por olhar para o `Caminho:` cabeçalho do campo. Este cabeçalho contém uma lista de todos os sistemas através do qual o artigo foi enviado em notação caminho bang.

Para distinguir e reconhecer as duplicatas artigos, artigos da Usenet dispor de uma identificação de mensagem (especificado no `Message-Id:` campo de cabeçalho), que combina o nome do site de postagem eo número de série em <*série@site*>.
Para cada artigo processado, o sistema de notícias registra esse ID em um *história* arquivo, contra o qual todos os recém-chegados artigos
culos são verificados.

O fluxo entre dois sites pode ser limitado por dois critérios. Por um lado, um artigo é atribuída uma distribuição (em
o `Distribuição:` campo de cabeçalho), que pode ser usado para confiná-la a um determinado grupo de sites. Por outro
Por outro lado, os grupos de notícias trocado pode ser limitado por ambos os sistemas de envio e recebimento. O conjunto de notícias
grupos e as distribuições de poder ser transmitida a um site geralmente são mantidos no *sys* arquivo.

O grande número de artigos normalmente requer que sejam feitas melhorias para o esquema acima. Na rede UUCP
obras, os sistemas de recolha de artigos ao longo de um período de tempo e combiná-los em um único arquivo, que é comprimido
e enviados para o site remoto. Isso é chamado *lotes*.

Uma técnica alternativa é a *ihave / sendme* protocolo que previne a duplicação de artigos de ser transferido, assim economizando banda da rede. Em vez de colocar todos os artigos em arquivos em lotes e enviá-los junto, apenas as identificações de mensagem
dos artigos são combinados em um gigante mensagem "ihave" e enviou para o site remoto. O site remoto lê este mes-
sábio, compara-lo ao seu arquivo histórico, e retorna a lista de artigos que quer em uma mensagem "sendme". Somente o requested artigos são enviados.

De ihave curso / sendme só faz sentido se envolve dois grandes sites que recebem notícias de vários inde-
ent alimenta cada, e que a votação de cada outro, muitas vezes suficiente para um fluxo eficiente de notícias.

Sites que estão na Internet em geral contam com o software TCP / IP que usa o Network News Transfer Protocolo (NNTP). NNTP é descrito na RFC-977, que é responsável pela transferência de notícias entre os servidores de notícias e fornece acesso aos usuários da Usenet único em máquinas remotas.

NNTP conhece três formas diferentes de transferência de notícias. Um deles é um tempo real versão do ihave / sendme, também

conhecido
como *empurrando* notícias. A segunda técnica é chamada *puxando* notícias, em que o cliente solicita uma lista de artigos em um newsgroup dado ou hierarquia que chegaram ao local do servidor após uma data especificada, e escolhe aqueles que
não pode encontrar em seu arquivo histórico. A terceira técnica é para newsreading interativo e permite que você ou sua notícia-leitor, para recuperar artigos de newgroups especificados, bem como postar artigos com informações de cabeçalho incompletas.

Em cada local, a notícia é mantido em uma hierarquia de diretórios abaixo */ Var / spool / news*, Cada artigo em um arquivo

separado, e cada
newsgroup em um diretório separado. O nome do diretório é composto do nome do grupo de notícias, com os componentes sendo o componente de caminho. Assim, os artigos são mantidos em comp.os.linux.misc */ Var / spool / news / comp / linux / misc*.
Os artigos em um newsgroup são atribuídos números na ordem de chegada. Este número serve como nome do arquivo.
O intervalo de números de artigos online no momento é mantido em um arquivo chamado *ativos*. Que ao mesmo tempo serve

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

como um
lista de newsgroups seu site sabe.

Como o espaço em disco é um recurso finito, você tem que começar jogando fora artigos depois de algum tempo.[123] Isso é

chamado
expirando. Geralmente, os artigos de certos grupos e hierarquias são terminou em um número fixo de dias após o seu chegar. Isto pode ser substituído pelo seu autor, especificando a data de expiração no `Expira em:` domínio da artigo cabeçalho.

Agora você tem informações suficientes para escolher o que ler em seguida. UUCP usuários devem ler sobre o C-Notícias no

Chap-
ter 21. Se você estiver usando uma rede TCP / IP, leia sobre NNTP no Capítulo 22. Se você precisar transferir moderados

123 Algumas pessoas afirmam que a Usenet é uma conspiração por vendedores de disco rígido e modem.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

quantidade de notícias sobre TCP / IP, o servidor descrito no capítulo que pode ser o suficiente para você.

Para instalar uma pesada
servidor direito a notícia de que pode lidar com grandes volumes de material, passam a ler sobre notícias da Internet no capítulo 23.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 21 - Notícias C

Um dos softwares mais populares para Netnews é C News. Ele foi projetado para sites que transmitem notícias mais links UUCP. Este capítulo irá discutir os conceitos centrais da C News, instalação básica e manutenção tarefas.

C News armazena seus arquivos de configuração em */ Notícias / etc*, Ea maioria dos seus binários são mantidos abaixo do */ Usr / lib / news /* di-
tório. Os artigos são mantidas abaixo */ Var / spool / news*. Você deve se certificar de que praticamente todos os arquivos nesses diretórios são
propriedade do usuário *notícias* ou grupo *notícias*. A maioria dos problemas surgem a partir de arquivos estão inacessíveis a C News. Use `su` para
se o usuário *notícias* antes de tocar em nada no diretório. A única exceção é o `setnewsids`
comando, que é usado para definir o ID de usuário real de alguns programas de notícias. Deve ser de propriedade da *root* e ter a setuid bit definido.

Neste capítulo, descrevemos todos os arquivos de configuração C notícias em detalhe e mostrar o que você tem que fazer para manter
seu site funcionando.

Cumprindo Notícias

Os artigos podem ser alimentados com C notícias de várias maneiras. Quando um usuário posta local, um artigo, o leitor geralmente as mãos
-lo para o `inews` comando, que completa a informação do cabeçalho. Notícias de sites remotos, seja ele um único arti-
cle ou todo um grupo, é dada ao `rnews` comando, que armazena na */ Var / spool / news / in.coming* di-
tório, de onde ele será pego em um momento posterior, `newsrun`. Com qualquer uma destas duas técnicas, no entanto, o artigo acabará por ser entregue ao `relaynews` comando.

Para cada artigo, o `relaynews` comando verifica primeiro se o artigo já foi visto no local por local
olhando para o ID da mensagem na *história* arquivo. Os artigos duplicados são descartados. Em seguida, `relaynews` olha para o
`Grupos de notícias:` linha de cabeçalho para saber se os pedidos de site local artigos de qualquer um desses grupos. Se isso acontecer, e
o grupo de notícias é listada na *ativos* arquivo, `relaynews` tenta armazenar o artigo no diretório correspondente no a área de spool de notícias. Se este diretório não existir, ele é criado. O ID do artigo é a mensagem é então registrado no *história* arquivo. Caso contrário, `relaynews` gotas do artigo.

Às vezes `relaynews` falha ao guardar um artigo de entrada, porque um grupo para o qual foi publicado não é listadas no seu *ativos* arquivo. Neste caso, o artigo é movido para o grupo de sucata.[124] `relaynews` também verifica obsoleto ou artigos misdated e rejeitá-los. lotes de entrada que não por qualquer outro motivo são movidos para */ Var / spool / news / in.coming / ruim*E uma mensagem de erro é registrado.

Depois disso, o artigo é retransmitida para todos os outros sites que as notícias pedido desses grupos, utilizando a especi- transporte
cados para cada site em particular. Para certificar-se de um artigo não é enviado para um site que já vi, cada destino local está marcada contra o artigo da `Caminho:` campo de cabeçalho, que contém a lista de sites que o artigo tenha atravessado Até agora, escrito no estilo bang UUCP caminho de roteamento de origem do estilo descrito no Capítulo 17, *Correio Eletrônico*. Se o
nome do site de destino não aparecem nessa lista, o artigo é enviado para ele.

C News é comumente usado para transmitir notícias entre sites UUCP, mas também é possível usá-lo em um NNTP ambiente. Para enviar notícias para um site remoto UUCP, quer em artigos ou um lote inteiro, `uux` é usado para executar o `rnews` comando no site remoto e alimentar o artigo ou lote para ele na entrada padrão. Consulte Capítulo 16, *Gerenciando UUCP Taylor*, Para obter mais informações sobre o UUCP.

Lotes é o termo usado para descrever o envio de pacotes grandes de artigos individuais em um único transporte. Quando lotes está habilitado para um determinado site, C notícias não envia qualquer artigo recebido imediatamente, em vez disso, ele

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

acrescenta
seu nome de caminho para um arquivo, geralmente chamado *site out.going / togo*. Periodicamente, um programa é executado a partir de um `crontab`
entrada pela `cron` programa, que lê este arquivo e feixes de todos os artigos listados em um ou mais arquivos, opcionalmente compactá-los e enviá-los para `rnews` no site remoto.[125]

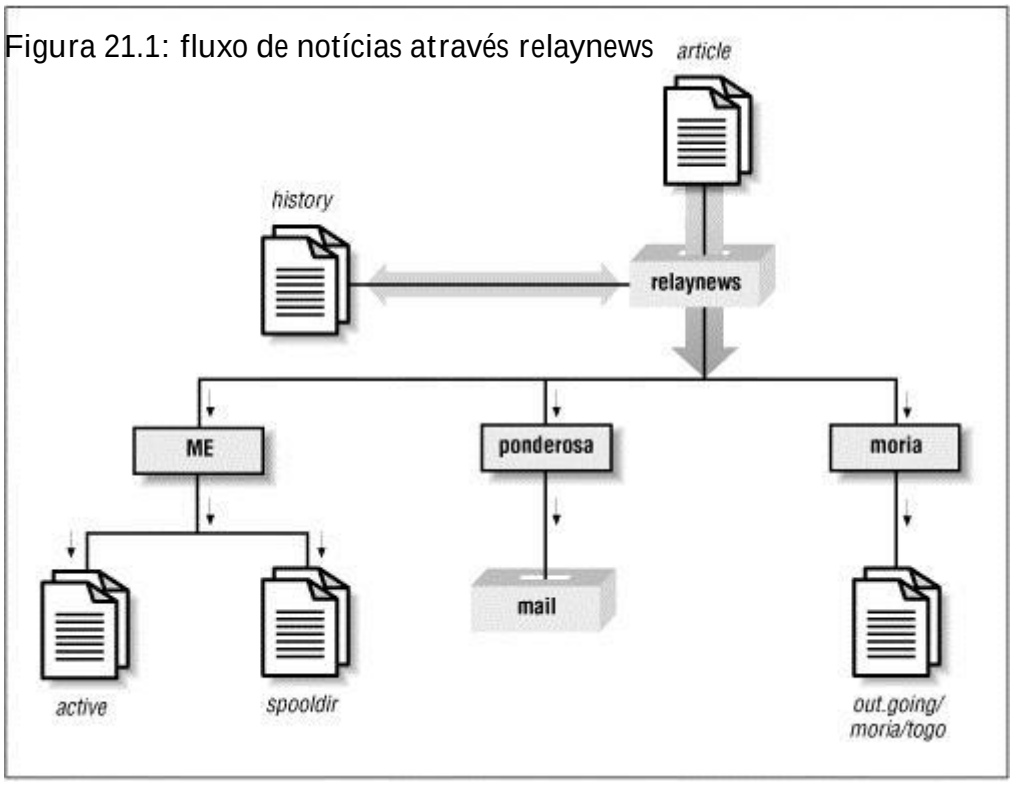
124 Pode haver uma diferença entre os grupos que existem no seu site e aqueles que o site está disposto a receber. Por exemplo, o lista de assinaturas pode especificar comp.all, que deverá enviar todos os newsgroups abaixo da hierarquia comp, mas em seu site, você pode não listar vários newsgroups comp na *ativos* arquivo. Artigos postados para os grupos serão movidas para a sucata.

125 Note-se que este deve ser o `crontab` de *notícias*; Permissões do arquivo não será mutilado.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Figura 21.1 shofoi o fluxo de notícias por meio de `relaynews`. Os artigos podem ser transmitidas para o site local (indicado por
ME), Para um site chamado *ponderosa* via e-mail e um site chamado *moria*, Para o qual dosagem é habilitado.

Figura 21.1: fluxo de notícias através relaynews



Instalação

C notícias devem estar disponíveis em um formato pré-embalados para qualquer distribuição Linux moderna, por isso a instalação será
fácil. Se não, ou se você quiser instalar a partir da distribuição do código fonte original, então é claro que você pode.[126] Não importa
como instalá-lo, você precisará editar o arquivos de configuração C News. Seus formatos são descritos na seguintes da lista:

sys

A *sys* controles de processo que newsgroups seu site recebe e encaminha. Nós discutimos isso em pormenor no seção seguinte.

ativos

Não é normalmente editado pela administração, contém instruções para lidar com artigos em cada grupo de notícias do site alças.

organização

Este arquivo deve conter o nome da sua organização, por exemplo, "Virtual Brewery, Inc." Em sua casa máquina, digite "site privado", ou qualquer outra coisa que você gosta. A maioria das pessoas não consideram o seu site corretamente
configurado se você não tiver personalizado o arquivo.

newsgroups

Este arquivo é uma lista de todas as notícias, com uma descrição de uma linha do propósito de cada um. Estas descrições
são freqüentemente utilizados por seu leitor ao exibir a lista de todos os grupos aos quais você está subdescrito.

mailname

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O nome do seu site, e-mail, por exemplo, *vbrew.com*.

126 Você pode obter a distribuição do código fonte C Notícias de seu home-site *ftp.cs.toronto.edu / Pub / news-c / c-news.tar.Z*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

whoami

O nome do seu site, para fins de notícias. Muitas vezes, o nome do site UUCP é usado, por exemplo, *vbrew*.

explist

Você provavelmente deve editar esse arquivo para refletir o seu tempo de expiração de newsgroups preferenciais especiais.
espaço em disco podem desempenhar um papel importante em suas escolhas.

Para criar uma hierarquia inicial de newsgroups, obtenha *ativos* e *newsgroups* arquivos do site que te alimenta.
Instalá-los em */ Notícias / etc*, Certificando-se que são de propriedade da *notícias* e têm um modo de 644, usando o `chmod` commando. Remova todos .* grupos do arquivo ativo e adicione-to.my site, site-to.feed, lixo e controle. O que .*
grupos são normalmente utilizados para a troca ihave / messages sendme, mas você deve incluí-los independentemente de você planeja usar ihave / sendme ou não. Em seguida, substituir todos os números no campo de segundo e terceiro *ativos* usando os seguintes comandos:

```
#  active.old ativa cp
#  sed 's / [0-9] * [0-9] * / 0000000000 00001 /'> active.old ativos
#  rm active.old
```

O segundo comando chama o `sed` stream editor. Esta invocação substitui duas seqüências de dígitos com uma corda de zeros ea cadeia `000001`, Respectivamente.

Finalmente, crie o diretório de spool de notícias e subdiretórios utilizados para a notícia de entrada e saída:

```
#  cd / var / spool
#  Notícias mkdir / news in.coming / news out.going / out.master
#  chown-R news.news notícias
#  chmod-R 755 notícias
```

Se você estiver usando pré-compilado locutores provenientes de uma distribuição diferente para o servidor de notícias você tem

C

execução, você pode descobrir que alguns esperam que o spool de notícias em */ Usr / spool / news* ao invés de */ Var / spool / news*. Se a sua
leitor parece não encontrar nenhum artigo, criar um link simbólico de */ Usr / spool / news* para */ Var / spool / news* como isso:

```
#  ln-sf / usr / spool / news / var / spool / news
```

Agora você está pronto para receber notícias. Observe que você não tem que criar o grupo de notícias individuais Directo

carretel

Ries. C News cria automaticamente listas de spool para qualquer grupo de notícias que recebe um artigo para, se não já existem.

Em particular, isso acontece com *todos* grupos a que um artigo foi cruzada lançada. Então, depois de um tempo, você vai encontrar o spool de notícias cheia de diretórios para newsgroups que você nunca tenha subscrito, como alt.lang.teco. Você pode impedir que isto tanto pela remoção de todos os grupos indesejados *ativos*Ou regularmente executado um script que remove todos os diretórios vazios abaixo */ Var / spool / news* (Excepto *out.going* e *in.coming*, É claro).

C News precisa de um usuário envie mensagens de erro e relatórios de status para. Por padrão, esta é *usenet*. Se você usar o defalha, você tem que configurar um alias para ele que encaminha todas as pessoas do seu e-mail para um ou mais responsáveis. Você pode
também substituir este comportamento configurando a variável de ambiente *NewsMaster* para o nome apropriado. Você tem que fazê-lo em *notícias*'S *crontab* arquivo, bem como toda vez que você chamar uma ferramenta administrativa manualmente, então instaleção um alias é provavelmente mais fácil. Mail aliases são descritos no Capítulo 18, *Sendmail*E Capítulo 19, *Obter Exim Up and Running*.

Enquanto estiver cortando */ Etc / passwd*, Certifique-se que cada usuário tem seu nome real no *pw_gecos* domínio da arquivo de senha (este é o quarto campo). É uma questão de netiqueta Usenet que o verdadeiro nome do remetente aparece em o `De:` campo do artigo. Claro, você vai querer fazer isso de qualquer maneira, quando você usa e-mail.

O sistema de arquivos

A *sys* arquivo, localizado na */ Notícias / etc*, Que controla as hierarquias receber e encaminhar para outros sites. Embora Existem ferramentas de manutenção do nome `addfeed` e `delfeed`, Achamos que é melhor manter este arquivo à mão.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A *sys* arquivo contém entradas para cada site ao qual você transmitir notícias, bem como uma descrição dos grupos que vai aceitar. A primeira linha é um *ME* entrada que descreve o seu sistema. É uma aposta segura para usar o seguinte:

```
ME: todos / todos::
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Você também tem que adicionar uma linha para cada site ao qual você feed de notícias. Cada linha tem esta aparência:

site[*/exclusões*]:*grouplist*[*/distlist*[]:*bandeiras*[:*cmds*]]

As inscrições podem ser continuada através newlines usando uma barra invertida (\) No final da linha a ser continuada. Um sinal de hash
(#) Denota um comentário.

site

Este é o nome do site da entrada se aplica. Um normalmente escolhe o nome do site UUCP para isso. Tem que haver uma entrada para o seu site na *sys* arquivo também, ou você não receberá nenhum artigo a si mesmo.

O nome do site especial *ME* denota o seu site. A *ME* entrada define todos os grupos que estão dispostos a loja localmente. Os artigos que não sejam acompanhadas por um *ME* linha vai para o grupo de lixo.

C News rejeita quaisquer artigos que já passaram por este local para evitar loops. C News faz isso assegurando que o nome do site local não aparecem na `Caminho:` do artigo. Alguns sites podem ser conhecido por uma série de nomes válidos. Por exemplo, alguns sites utilizam o seu nome de domínio totalmente qualificado no
Neste domínio, ou um apelido como `notícias.`*site.domain*. Para assegurar o loop funciona o mecanismo de prevenção, é importante para adicionar todos os aliases para a lista de exclusão, separando-os por vírgulas.

Para a entrada de aplicação para o site *moria*, Por exemplo, o *site* campo deverá conter *moria / moria.orcnet.org*. Se *moria* Foram também por um apelido de *news.orcnet.org*, Então a nossa *site* campo deverá conter *moria / moria.orcnet.org, news.orcnet.org*.

grouplist

Esta é uma lista de assinaturas de vírgulas de grupos e hierarquias para este site específico. Uma hierarquia pode ser especificado dando prefixo da hierarquia (como comp.os para todos os grupos cujos nomes começam com esse prefixo), seguido opcionalmente a palavra-chave todos (por exemplo comp.os.all).

Você pode excluir uma hierarquia ou grupo de encaminhamento, precedendo-a com uma exclamação. Se um newsgroup é verificada em relação a lista, a mais longa partida se aplica. Por exemplo, se *grouplist* contém essa lista:

```
! Comp comp.os.linux, comp.folklore.computers
```

sem grupos da hierarquia comp exceto comp.folklore.computers e todos os grupos abaixo comp.os.linux serão alimentados a esse site.

Se as solicitações de site para ser encaminhado todas as notícias que você recebe mesmo, entra *todos* como *grouplist*.

distlist

Este valor é o deslocamento do *grouplist* por uma barra e contém uma lista de distribuições deverão ser enviadas. Novamente, você poderá excluir determinadas distribuições precedendo-os com um ponto de exclamação. Todos os distribuições são indicados por *todos*. Omitindo *distlist* implica em uma lista de *todos*.

Por exemplo, você pode usar uma lista de distribuição de *todos,! local* para evitar que notícias destinado somente para uso local de
sendo enviadas para locais remotos.

Normalmente existem pelo menos duas distribuições: *mundo*, Que muitas vezes é a distribuição padrão usada quando nenhum é especificado pelo usuário, e *local*. Pode haver outras distribuições que se aplicam a uma determinada região, estado, país, etc Finalmente, há duas distribuições utilizadas pela C notícias só, estes são *sendme* e *ihave*, E são usados para o sendme / protocolo ihave.

O uso de distribuições é um assunto de debate. O campo de distribuição em um artigo de notícias podem ser criados de forma arbitrária,
mas para uma distribuição para ser eficaz, a servidores de notícias na rede deve conhecê-lo. Algumas notícias misbehaving-leitores criar distribuições falso, simplesmente assumindo a hierarquia do newsgroup de nível superior do artigo-destinação é uma distribuição razoável. Por exemplo, se poderia supor comp ser uma distribuição razoável utilizar durante o lançamento para o newsgroup comp.os.linux.networking. Distribuições que se aplicam a regiões são muitas vezes causacapaz, também, pois a notícia poderá viajar para fora de sua região quando enviados através da Internet.[127] Distributions aplicação

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

a uma organização, no entanto, são muito significativos, como por exemplo, para impedir que informações confidenciais saiam da
rede da empresa. Este propósito, entretanto, é geralmente melhor servido através da criação de um grupo de notícias separado ou hie-
chy.

127 Não é incomum para um artigo publicado em dizer, em Hamburgo, para ir para Frankfurt, via *reston.ans.net* na Holanda, ou mesmo através de algum site em os EUA

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

bandeiras

Esta opção descreve certos parâmetros para a alimentação. Pode ser vazia ou uma combinação das seguintes características:

`F`

Este indicador permite o processamento em lotes.

`f`

Isso é quase idêntico ao `F` bandeira, mas permite News C para calcular o tamanho dos lotes de saída mais precisamente, e provavelmente deve ser usado de preferência.

`I`

Esta opção faz o C News produzir uma lista de artigos adequados para uso por ihave / sendme. modificações adicionais-ções para o *sys* e *batchparms* arquivo são necessários para habilitar sendme / ihave.

`n`

Isso cria arquivos em lote de clientes ativos, como transferência de NNTP `nntpxmit` (Ver Capítulo 22, *NNTP e o Daemon nntpd*). Os arquivos em lote conter o nome do artigo, juntamente com o seu ID da mensagem.

`L`

Isto diz-C notícias para transmitir apenas os artigos destacados em seu site. Esta bandeira pode ser seguido por um número decimal
número *n*, Que faz artigos de transferência C notícias postadas apenas dentro *n* lúpulo a partir do seu site. Notícias de C-termines o número de saltos da *Caminho:* de campo.

`u`

Isto diz-C notícias para artigos lote apenas de grupos moderado.

`m`

Isto diz-C notícias para artigos lote apenas de grupos moderados.

Você pode usar no máximo uma das `F`,`f`,`I`Ou `n`.

cmds

Este campo contém um comando que será executado para cada artigo, a menos que você permitir que lotes. A artigo será alimentado com o comando na entrada padrão. Isso deve ser usado para a alimentação muito pequena só; ou-Do contrário, a carga em ambos os sistemas será muito alto.

O comando padrão é:

`uux - r-z` *sistema remoto*`! Rnews`

Isso chama `rnews` no sistema remoto, alimentando-o artigo sobre a entrada padrão.

O caminho de pesquisa padrão para os comandos dados neste campo é */ Bin: / usr / bin: / usr / lib / news / lote*. O último diretório contém uma série de shell scripts cujos nomes começam com `via`, Que são brevemente descritos mais adiante neste capítulo.

Se a dosagem é ativado através de um dos `F`,`f`,`I`Ou `n` bandeiras, C News espera encontrar um nome neste campo, em vez de um comando. Se o nome do arquivo não começar com uma barra (/), é assumido como sendo relativo ao */ Var / spool / news / out.going*. Se o campo estiver vazio, o padrão é *remote-system/togo*. O arquivo deverá estar em o mesmo formato que o *remote-system/togo* arquivo e contém uma lista de artigos para transmitir.

Ao configurar C News, você provavelmente terá de escrever o seu próprio *sys* arquivo. Aqui está um arquivo de amostra para *vbrew.com*, Da qual você pode copiar o que você precisa:

```
# Nós tomamos o que eles nos dão.
ME: todos / todos::
# Nós enviamos tudo o que recebem para moria, com exceção de locais e
# Cervejaria artigos relacionados. Usamos lotes.
moria / moria.orcnet.org:! todos, para, to.moria / todos os locais, cervejaria! f:
# Comp.risks Nós mail para jack@ponderosa.uucp
ponderosa: comp.risks / all: jack@ponderosa.uucp rmail
# Nadar recebe uma alimentação menor
nadar / swim.twobirds.com: rec.humor.oracle comp.os.linux, / tudo, local! f:
# Log-mail artigos de mapa para processamento posterior
usenet-mapas: comp.mail.maps / all: F: / var / spool / uumaps trabalho / / lote
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O arquivo ativo

A *ativos* arquivo está localizado na */ Etc /*E listas de todos os grupos conhecidos em seu site e os artigos online no momento.

Você
raramente terá que tocá-lo, mas explicá-lo mas, por causa da conclusão. Entradas ter os seguintes
forma:

newsgroup perm baixa alta

newsgroup é o nome do grupo. *baixa* e *alta* são os números mínimo e máximo de artigos disponíveis no momento.
Se nenhum estiver disponível no momento, *baixa* é igual a *alta*1.

Pelo menos é o que o *baixa* campo é destinado a fazer. No entanto, para a eficiência, C notícias não atualização neste campo.

Este
não seria uma perda tão grande se não houvesse locutores que dependem dele. Por exemplo, `trn` verifica esse campo para
ver se ele pode limpar todos os artigos da sua base de discussão. Para atualizar o *baixa* campo, portanto, você tem que executar o
`updatemin` comandos regularmente (ou, em versões anteriores do C News, o `upact` script).

permanente é um parâmetro que detalha o acesso dos usuários são atribuídos ao grupo. Demora um dos seguintes valores:

y

Usuários podem enviar mensagens para este grupo.

n

Os usuários não têm permissão para enviar mensagens para este grupo. No entanto, o grupo ainda pode ser lido.

x

Este grupo foi desativada localmente. Isso acontece às vezes, quando os administradores de notícias (ou os seus superiores) se ofendem com artigos postados a determinados grupos.

Os artigos recebidos para este grupo não são armazenados localmente, apesar de serem enviadas para os sites que rebusca-los.

m

Isto denota um grupo moderado. Quando um usuário tenta postar neste grupo, um leitor inteligente notiFIES-la de presente e mandar o artigo para o moderador vez. O moderador do endereço é retirado do *moderadores* arquivo em */ Var / lib / news*.

=grupo real

Isto marca *newsgroup* como sendo um alias local para outro grupo, ou seja, *grupo real*. Todos os artigos postados *newsgroup* será redirecionado para ele.

Em C News, você geralmente não precisa acessar o arquivo diretamente. Os grupos podem ser adicionados ou excluídos

localmente usando
`addgroup` e `delgroup` (Consulte a seção "Ferramentas de manutenção e tarefas" mais adiante neste capítulo). A *newgroup*
mensagem de controle adiciona um grupo para toda a Usenet, enquanto um *rmgroup* mensagens, apaga um grupo. *Nunca envie essa mensagem mesmo!* Para obter instruções sobre como criar um grupo de notícias, ler as publicações mensais
news.announce.newusers.

A *active.times* arquivo está intimamente relacionada com a *ativos* arquivo. Sempre que um grupo é criado, C News registra uma

mensagem
este arquivo contém o nome do grupo criado, a data de criação, se isso foi feito por um *newgroup* conmensagem de controle ou localmente, e quem fez isso. Isto é conveniente para locutores que pode notificar o usuário de qualquer re-
Recentemente criou grupos. Também é usado pelo `NEWGROUPS` comando de NNTP.

Artigo Lotes

lotes notícias seguem um formato especial, que é o mesmo para B Notícias, Notícias, C e DCI. Cada artigo é precedida
por uma linha como esta:

`#! rnews` *contagem*

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

contagem é o número de bytes no artigo. Quando você usa compressão de lote, o arquivo resultante é comprimida como uma todo e precedida por outra linha, indicado pela mensagem a ser usado para descompactar. O padrão de compressão-ferramenta de Sion é comprimir, que é marcado por:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
#! cunbatch
```

Às vezes, quando o servidor envia notícias lotes através do software de correio que remove o oitavo bit de todos os dados, um lote comprimidos podem ser protegidos usando o que chamamos *C7-codificação*; Destes lotes será marcado por `c7unbatch`.

Quando um lote é alimentado `rnews` no site remoto, ele verifica para estes marcadores e processos de apro-lote diatamente. Alguns sites também usam outras ferramentas de compressão, como `gzip`, E preceder seus arquivos compactado com a palavra
`zunbatch` em vez disso. C Notícias não reconhece cabeçalhos fora do padrão como estes, você tem que modificar a fonte para apoiá-los.

Em C News, lotes artigo é realizada por */ Usr / lib / news lote / sendbatches*, Que tem uma lista de artigos o *site / togo* arquivo e coloca-los em vários newsbatches. Ele deve ser executado uma vez por hora, ou até mais freqüentemente, dependendo do volume de tráfego. Sua operação é controlada pela *batchparms* arquivo em */ Var / lib / news*. Este arquivo descreve o tamanho de lote máximo permitido para cada site, a compressão de lotes e opcionais programa a ser utilizada, bem como o transporte para entregá-la para o site remoto. Você pode especificar parâmetros de lotes em um
base por site, bem como um conjunto de parâmetros padrão para os sites não são explicitamente mencionadas.

Ao instalar o C News, você provavelmente irá encontrar um *batchparms* arquivo na sua distribuição que contém uma razão-entrada padrão capaz, por isso há uma boa chance de que você não tem que tocar o arquivo. Apenas no caso, nós descrevemos a sua
formato. Cada linha consiste de seis campos, separados por espaços ou tabulações:

site tamanho máximo de transporte muncher batcher

site

> *site* é o nome do site para o qual a entrada se aplica. A *Togo* arquivo para esse site deve residir em *out.going / togo* abaixo do spool de notícias. Um nome de site da */ Default /* denota a entrada padrão e é combinar qualquer local não especificado diretamente com uma entrada única para ele.

tamanho

> *tamanho* é o tamanho máximo dos lotes artigo criado (antes da compressão). Para artigos únicos maiores que isso, C News faz uma exceção e coloca cada um em um único lote por si só.

max

> *max* é o número máximo de lotes criados e programados para a transferência de lotes antes de tendas para este determinado site. Isso é útil no caso de o local remoto deve ser para baixo por um longo tempo, porque impede C notícias de desordenar seus diretórios spool UUCP com zilhões de newsbatches.
>
> C News determina o número de lotes na fila usando o `queuelen` script em */ Usr / lib / news /*. Se você instalou C notícias em um formato pré-embalados, o script não deve precisar de qualquer edição, mas se você optar por usar um sabor diferente de diretórios de spool, por exemplo, Taylor UUCP, você pode ter que escrever seus próprios. Se você não se importa com o número de arquivos de spool (porque você é a única pessoa que usa
> seu computador e você não escreve artigos por megabyte), você pode substituir o conteúdo do script por um simples `exit 0` declaração.

batcher

> A *batcher* campo contém o comando usado para a produção de um lote da lista de artigos no *Togo* arquivo. Para regular feeds, isto é, normalmente `batcher`. Para outros fins, batchers alternativa pode ser pro-indicadas. Por exemplo, o protocolo ihave / sendme requer a lista de artigos para ser transformado em *ihave* ou *sendme* mensagens de controle, que são enviadas para o to.site newsgroup. Isso é realizado por `batchih` e `batchsm`.

pessoa que mastiga ruidosamente

> A *pessoa que mastiga ruidosamente* campo especifica o comando de compressão. Normalmente, isso é compcun, um script que produz
> um lote de comprimidos.[128] Em alternativa, suponha que você criar um muncher que usa `gzip`, Diz gzipcun (Note que você tem que escrever mesmo). Você tem que se certificar de que `descompactar` no site remoto é patch para reconhecer arquivos compactados com `gzip`.
>
> Se o site remoto não tem um `descompactar` comando, você pode especificar `nocomp`, Que não fazer qualquer compressão.

[128] Como enviado com C News, usa compcun comprimir com a opção de 12 bits, já que este é o menor denominador comum para a maioria dos sites.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Você pode produzir uma cópia do roteiro, digamos compcun16, para o qual você utilizar a compressão de 16 bits. A melhoria não é muito impressionante, embora.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

transporte

O último campo, *transporte*, Descreve o transporte a ser utilizado. Uma série de comandos padrão para diferentes ent transportes estão disponíveis; seus nomes começam com `via.sendbatches` passa-lhes o destino sitename na linha de comando. Se o *batchparms* entrada não é */ Default /*,`sendbatches` deriva a sitename da *site* campo, retirando-lhe qualquer coisa, inclusive após o primeiro ponto ou barra. Se o *batchparms* entrada é */ Default /*, Os nomes de diretório em *out.going* são utilizados.

Para executar lotes para um site específico, use o seguinte comando:

c su-news "/ usr / lib / news / lote / site sendbatches"

Quando chamado sem argumentos, `sendbatches` lida com todas as filas batch. A interpretação de "tudo" depende sobre a presença de uma entrada padrão na *batchparms*. Se um for encontrado, todos os diretórios em */ Var / spool / news / out.going* são
marcada, caso contrário, `sendbatches` percorre todas as entradas *batchparms*, O processamento apenas os sites encontrados ali. Note-se que `sendbatches`, Quando a digitalização do *out.going* diretório, leva apenas os diretórios que contêm sem pontos ou sinais (@) Como nomes de sites.

Existem dois comandos que usam `uux` para executar `rnews` no sistema remoto: `viauux` e `viauuxz`. A
este define a *-Z* Sinalizar para `uux` para manter as versões antigas de retornar mensagens de sucesso para cada um dos artigos entregues.
Outro comando, `viamail`, Envia lotes artigo para o usuário *rnews* no sistema remoto via correio. Claro,
Isto requer que o sistema remoto de alguma forma todos os feeds e-mail para *rnews* ao seu sistema de notícias locais. Para uma completa
lista desses transportes, referem-se ao *newsbatch* manual de página.

Todos os comandos dos três últimos campos devem estar localizados em qualquer *out.going / site* ou */ Usr / news / lib / lote*. A

maioria dos
eles são scripts, você pode facilmente adaptar novas ferramentas para suas necessidades pessoais. Eles são invocados através de tubos. A
lista de artigos é alimentado ao batcher na entrada padrão, que produz o lote na saída padrão. Este é canalizada
no muncher, e assim por diante.

Aqui está um arquivo de exemplo:

```
# Arquivo batchparms para a cervejaria
# Site        | Tamanho   |    | Batcher | Muncher   | Transporte
              Max
#-------------+--------+-------+---------+-------- ---+-----------
/ Default /     100000  22      batcher   compcun     viauux
nadar            10000  10      batcher   nocomp      viauux
```

Vencer Notícias

Em B News, validade precisa ser executada por um programa chamado `expirar`, Que fez uma lista de grupos como argumentos, juntamente com uma especificação do tempo após o qual os artigos tiveram de ser expirado. Para se ter diferentes hierarquias
expiram em diferentes momentos, você tinha que escrever um script que invocou `expirar` para cada um deles separadamente. C News
oferece uma solução mais conveniente. Em um arquivo chamado *explist*, Você pode especificar grupos de notícias e intervalos de expiração.
Um comando chamado `doexpire` geralmente é executado uma vez por dia a partir de `cron` e processos de todos os grupos de acordo com esta
lista.

Ocasionalmente, você pode querer guardar artigos de determinados grupos, mesmo após terem sido expirado, por exemplo, você pode querer manter os programas lançados comp.sources.unix. Isso é chamado *arquivamento.explist* permite que você para marcar grupos para arquivamento.

Uma entrada em *explist* parecido com este:

grouplist perm arquivo vezes

grouplist é uma lista separada por vírgulas de grupos de notícias para que a entrada se aplica. Hierarquias podem ser

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

especificados por
dando o prefixo do nome do grupo, opcionalmente adicionados com *todos*. Por exemplo, para uma entrada aplicáveis a todos os grupos
abaixo comp.os, introduza comp.os ou comp.os.all.

Quando *expirando* notícias de um grupo, o nome é verificado em todas as entradas *explist* na ordem dada. O primeiro entrada correspondente aplica. Por exemplo, para jogar fora a maioria dos comp depois de quatro dias, excepto para comp.os.linux.announce, que pretende manter durante uma semana, você simplesmente tem uma entrada para o último, que especifica um período de validade de sete dias, seguido por um período de validade para comp, que especifica quatro dias.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A *permanente* Detalhes do campo, se a entrada se aplica a moderado, sem moderador, ou qualquer grupo. Ele pode tomar os valores *m*,*u*,
ou *x*, Que denotam moderado, sem moderador, ou qualquer outro tipo.

O terceiro campo, *vezes*, Geralmente contém apenas um número único. Este é o número de dias após o qual os artigos caduca se não tiverem sido atribuída uma data de expiração artificial em um `Expira em:` campo no cabeçalho do artigo. Nota que este é o número de dias contados da sua *chegada* no seu site, e não a data de postagem.

A *vezes* campo pode, no entanto, ser mais complexa do que isso. Pode ser uma combinação de até três números de sepa- avaliado entre si por traços. O primeiro indica o número de dias que têm de passar antes que o artigo é considerado um candidato para a expiração, mesmo se o `Expira em:` campo teria expirar já. Raramente é de uso ful para usar um valor diferente de zero. O segundo campo é o número padrão mencionado anteriormente dias depois que será expirado. O terceiro é o número de dias depois que um artigo será expirado incondicionalmente, independentemente de ter um `Expira em:` campo ou não. Se apenas o número do meio é dado, os outros dois ter valores padrão. Estes podem ser especificados usando a entrada especial */ Limites /*, Que é descrito um pouco mais tarde.

O quarto campo, *Arquivo*, Indica se o grupo de notícias é para ser arquivado e onde. Se nenhum arquivo é in- tendiam, um traço deve ser usado. Caso contrário, você usar um caminho completo (apontando para um diretório) ou um sinal de arroba
(@). A arroba denota o diretório do arquivo padrão, que deve então ser dada a `doexpire` usando o *-Um* flag na linha de comando. Um diretório do arquivo deve ser de propriedade da *notícias*. Quando `doexpire` arquivos de um artigo
de dizer, comp.sources.unix, ele armazena no diretório comp / fontes unix / abaixo do diretório do arquivo, criando se for necessário. O diretório do arquivo em si, no entanto, não será criado.

Existem duas entradas especiais em seu *explist* arquivo que `doexpire` depende. Em vez de uma lista de grupos, eles tenham as palavras-chave */ Limites /* e */ Expirado /*. A */ Limites /* entrada contém os valores padrão para os três valores de o *vezes* campo descrito anteriormente.

A */ Expirado /* campo determina quanto tempo C News vai agarrar linhas no *história* arquivo. C notícias não irá remover uma linha do arquivo histórico uma vez que o artigo correspondente (s) foram vencidos, mas vai agarrar-lo no caso de um duplicado deve chegar após essa data. Se você é alimentado por um único site, você pode manter esse valor pequeno. Caso contrário, uma
Duas semanas é aconselhável em redes UUCP, dependendo do atraso que a experiência com artigos de esses sites.

Aqui está um exemplo *explist* arquivo com bastante apertado intervalos de validade:

```
# Manter a linha da história por duas semanas. Nenhum artigo recebe mais de três meses
/ Expirado /                    x       14      -
/ Limites /                     x       0-1-90  -
# Grupos que querem manter mais do que o resto
comp.os.linux.announce          m       10      -
comp.os.linux                   x       5       -
alt.folklore.computers          u       10      -
rec.humor.oracle                m       10      -
soc.feminism                    m       10      -
# Arquivo de fontes grupos *.
comp.sources, alt.sources       x       5       @
# padrões para os grupos de
tecnologia                      x       7       -
comp, sci
# Suficiente para um fim de     x       4       -
semana prolongado
Discussão misc,                 x       1       -
# Jogar fora lixo rapidamente
lixo
# mensagens de controle são de pouco interesse,
também                                          -
controle                        x       1
# Catch-entrada para todos o resto
todos                           x       2       -
```

Vencer apresenta vários problemas potenciais. Uma delas é que o seu leitor poderá contar com o terceiro campo do *ativos* arquivo descrito anteriormente, que contém o número da linha menor artigo. Quando os artigos que termina, C Notícias não atualizar este campo. Se você precisa (ou quer) ter esse campo representam a situação real, que você precisa

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

executar um programa chamado `updatemin` após cada ensaio de `doexpire`. (Em versões mais antigas do C News, um script chamado
`upact` fez isso.)

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

C notícias não terminam por varredura diretório do grupo de notícias, mas simplesmente verifica o *história* arquivo se o artigo é devido a expiração.[129] Se o seu arquivo histórico de alguma forma fica fora de sincronia, os artigos podem ser em torno de seu disco para sempre
porque C News literalmente esquecido.[130] Você pode reparar isso usando o `addmissing` script em */ Usr / news / lib / maint*, Que irá adicionar artigos em falta no *história* arquivo ou `mkhistory`, Que recria todo o arquivo a partir do zero. Não se esqueça de tornar-se usuário *notícias* antes de invocá-lo, senão você acabará com um *história* arquivo ilegível por C News.

Diversos arquivos

Há uma série de arquivos que controlam o comportamento do C News, mas não são essenciais. Todos eles residem em */ Notícias / etc*. Nós descrevê-los brevemente aqui:

newsgroups

Este é um arquivo companheiro de *ativos* que contém uma lista de cada nome de newsgroup, juntamente com uma linha-de-
crição do seu tema principal. Este arquivo é atualizado automaticamente quando recebe uma notícia C *checknews* con-controle da mensagem.

localgroups

Se você tem um monte de grupos locais, você pode manter Notícias de C queixando-los cada vez que você re-ceive um `checkgroups` mensagem, colocando seus nomes e descrições neste arquivo, como fariam aparecem em *newsgroups*.

mailpaths

Este arquivo contém o endereço do moderador para cada grupo moderado. Cada linha contém o nome do grupo seguido pelo moderador do endereço de email (compensado por um guia).

Duas entradas especiais são fornecidos por omissão: *espinha dorsal* e *Internet*. Ambos fornecem, em notação de caminho-bang, a
caminho para o local mais próximo da coluna vertebral e no local que compreende RFC-822 endereços de estilo (user @ host). O padrão
entradas são:

```
Internet            espinha dorsal
```

Você não tem que mudar o *Internet* entrada se tiver `exim` ou `sendmail` instalados, pois eles entendem RFC-822 de resolução.

A *espinha dorsal* entrada é usada sempre que um usuário envia a um grupo moderado cujo moderador não estiver listado explicitamente.
Se o nome do newsgroup é alt.sewer eo *espinha dorsal* entrada contém caminho!% s, C News vai enviar o artigo para caminho! esgoto alternativo, esperando que a máquina de espinha dorsal é capaz de transmitir o artigo. Para descobrir qual o caminho a ser usado,
pedir a notícia-admin no site que te alimenta. Como último recurso, você também pode usar uunet.uu.net!% S.

distribuições

Esse arquivo não é realmente um arquivo C News, mas é usado por alguns leitores e `nntpd`. Ele contém a lista de dis-ções reconhecidas pelo seu site e uma descrição da sua (prevista) efeitos. Por exemplo, Virtuais cervejaria tem o seguintes arquivos:

```
mundo          em todo o mundo
local          Apenas locais para este site
nl             Holanda só
mugnet         MUGNET apenas
fr             França só
de             Alemanha só
cervejaria     Virtual única cervejaria
```

log

Este arquivo contém um registro de todas as atividades de C News. É abatido regularmente, executando `NewsDaily`; Cópias dos antigos
arquivos de log são mantidos em *log.o*,*log.oo*, Etc

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

129 O artigo data de chegada é mantido no campo do meio da linha de história e de dados em segundos desde 1 de janeiro de 1970.
130 Eu não sei *por* isso acontece, mas ele faz de vez em quando.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Este é um registo de todas as mensagens de erro criado por C News. Estas mensagens não incluem os registros de artigos junked devido
de serem enviados para um grupo inválido errada ou erros de outros usuários. Este arquivo é enviado para o newsmaster (*usenet* por
padrão) automaticamente pelo `NewsDaily` se não for encontrada vazia.

errlog é eliminada por `NewsDaily`.*errlog.o* mantém cópias antigas e companheiros.

batchlog

Este arquivo registra todas as pistas de `sendbatches`. Geralmente é de escasso interesse. É também com a participação de `notícias diária`.

watchtime

Este é um arquivo vazio criado cada vez `Newswatch` é executado.

Controle Mensagens

O protocolo de notícias da Usenet sabe uma categoria especial de objectos que evocam respostas certas ou ações do novidades do sistema. Estes são chamados *controle* mensagens. Eles são reconhecidos pela presença de um *Controle:* campo na cabeçalho do artigo, que contém o nome da operação de controle a ser realizado. Existem vários tipos de eles, que são manipulados pelo shell scripts localizados em */ Usr / lib / news / CTL*.

A maioria destas mensagens realizar sua ação automaticamente no momento do artigo é processado por C sem notícias notificando o newsmaster. Por padrão, apenas *checkgroups* mensagens serão entregues ao newsmaster, mas você pode mudar isso editando os scripts.

O cancelamento Mensagem

A mensagem mais conhecida é *cancelar*, Com o qual um usuário pode cancelar um artigo enviado anteriormente. Isso efetivamente
remove o artigo dos diretórios de spool, se ele existir. A *cancelar* mensagem é encaminhada para todos os sites que re- notícias necessário para receber os grupos afetados, independentemente de o artigo já tem sido visto. Isso leva em conta a possibilidade de que o artigo original foi adiado sobre a mensagem de cancelamento. Alguns sistemas de notícias tems permitem aos utilizadores cancelar mensagens de outras pessoas, isto é, naturalmente, um definitivo não-não.

newgroup e rmgroup

Duas mensagens de lidar com a criação ou remoção de grupos de discussão são os *newgroup* e *rmgroup* mensagens. -Notícias grupos abaixo do "normal" hierarquias podem ser criadas somente após uma discussão e votação foi realizada entre leitores da Usenet. As regras aplicáveis à hierarquia alt permitir algo próximo a anarquia. Para mais infor- ção, ver os lançamentos regulares em news.announce.newusers e news.announce.newgroups. Nunca envie um *novo grupo* ou *rmgroup* Mensagem sozinho, a menos que você definitivamente sabe que você está permitido.

O checkgroups Mensagem

checkgroups mensagens são enviadas por administradores de notícias para fazer todos os locais dentro de uma rede sincronizem seus *ac-*
tiva arquivos com as realidades da Usenet. Por exemplo, comerciais na Internet Service Providers pode enviar um tal mensagem para os sites de seus clientes. Uma vez por mês, o "oficial" *checkgroups* mensagem para os grandes hierarquias é colocada comp.announce.newgroups pelo seu moderador. No entanto, é publicado como um artigo comum, não como um con- controle da mensagem. Para executar o *checkgroups* operação, salve este artigo em um arquivo, digamos */ Tmp / check*, Remova-a cada
coisa até o início da mensagem de controle em si, e fornecê-lo ao *checkgroups* script usando o seguinte comando:

```
#  c su-news "/ usr / lib / news / CTL / checkgroups" </ tmp / seleção
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Isto irá atualizar o seu *newsgroups* arquivo da nova lista de grupos, adicionando os grupos constantes *localgroups*. A idade *newsgroups* arquivo será movido para *newsgroups.bac*. Note-se que postaram a mensagem localmente raramente funciona, ser-
causa `inews`, O comando que aceita artigos e posts dos usuários, se recusa a aceitar que um artigo de grande porte.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Se C News encontra discrepâncias entre as *checkgroups* lista e os *ativos* arquivo, ele gera uma lista de comandos que traria o seu site atualizado e e-mails para o administrador de notícias.

A saída normalmente é assim:

```
De notícias dom 30 jan 1994 16:18:11
Date: Fri, 30 Jan 94 16:18 MET
De: news (notícias Subsystem)
Para: usenet
Assunto: Problemas com o arquivo ativo
Os seguintes grupos de notícias não são válidas e devem ser removidos.
        arte-alt.ascii
        bionet.molbio.gene-org
        comp.windows.x.intrisics
        de.answers
Você pode fazer isso executando os seguintes comandos:
         / Usr / lib / news / maint / delgroup arte alt.ascii
         / Usr / lib / news maint / delgroup bionet.molbio.gene-org
         / Usr / news / lib / maint / delgroup comp.windows.x.intrisics
         / Usr / news / lib / maint / delgroup de.answers
Os seguintes grupos de notícias estavam faltando.
        comp.binaries.cbm
        comp.databases.rdb
        comp.os.geos
        comp.os.qnx
        comp.unix.user-friendly
        misc.legal.moderated
        news.newsites
        soc.culture.scientists
        talk.politics.crypto
        talk.politics.tibet
```

Quando você receber uma mensagem como essa a partir do seu sistema de notícias, não acredito que automaticamente.

Dependendo de quem
enviou à *checkgroups* mensagem, que pode faltar alguns grupos ou até mesmo hierarquias todo, você deve ter cuidado com remover quaisquer grupos. Se você encontrar grupos estão listadas como desaparecidas que pretende realizar em seu site, você tem que adicionar
los utilizando o `addgroup` script. Salvar a lista de grupos que faltava para um arquivo e fornecê-lo ao pequeno seguintes script:

```
#! / Bin / sh
#
WHOIAM = whoami `
if ["$ WHOIAM!" = "news"]
em seguida,
        echo "Você deve correr $ 0 como" notícias "usuário"> & 2
        saída 1
fi
#
cd / usr / lib / news
enquanto lê grupo; fazer
    se grep-si "^ $ [grupo [: space :]].* moderado" newsgroup, então
        mod m =
    mais
        mod y =
    fi
    / Usr / lib / news maint / addgroup $ grupo $ mod
feito
```

sendsys, versão e senduuname

Finalmente, há três mensagens que podem ser usadas para descobrir a topologia da rede. Estes são *sendsys*, *versão*E *senduuname*. Eles causam C notícias para retornar a *sys* ficheiro para o remetente, bem como uma versão de software

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

seqüência ea saída de `uuname`, Respectivamente. C News é muito lacônica sobre *versão* mensagens, ele retorna um simplo, sem adornos `C`.

Novamente, você deve *nunca* emitir tal mensagem, a menos que você tenha a certeza de que não pode deixar o seu (regional) rede. Respostas para a *sendsys* mensagens pode rapidamente derrubar uma rede UUCP.[131]

C notícias em um ambiente NFS

Uma forma simples de distribuir notícias dentro de uma rede local é manter todas as notícias em um host central e exportar a

rele-

Vant diretórios via NFS, para que leitores de notícias pode digitalizar os artigos diretamente. A sobrecarga envolvida na recuperação e rosqueamento artigos é significativamente inferior NNTP. NNTP, por outro lado, ganha em uma rede heterogênea, trabalho onde o equipamento varia muito entre os hosts, ou onde os usuários não têm contas equivalentes no servidor máquina.

Quando você usa NFS, artigos publicados em um servidor local tem que ser encaminhado para a máquina central, pois acesso ing arquivos administrativos poderiam expor o sistema a condições de corrida que deixar os arquivos inconsistentes. Além disso, você pode querer proteger a sua área de spool de notícias, exportando-o somente leitura, que também requer o encaminhamento
para a máquina central.

C News trata esta configuração da máquina central de forma transparente para o usuário. Quando você publica um artigo, o newsreader geralmente chama `inews` para injetar o artigo para o sistema de notícias. Esse comando executa uma série de controlo do artigo, conclui o cabeçalho, e verifica o arquivo *servidor* em */ Notícias / etc*. Se esse arquivo existir e contiver um nome diferente do nome do host local, `inews` é chamado em que servidor hospedeiro via `rsh`. Desde o `em ews` script usa uma série de comandos binários e arquivos de suporte da C News, você tem quer ter C News instalado localmente ou montar o software do servidor de notícias.

Para o `rsh` invocação para funcionar adequadamente, cada usuário que posta notícias deve ter uma conta equivalente no sistema de servidor, ou seja, aquele ao qual ela pode entrar sem ser solicitado para uma senha.

Certifique-se que o hostname dado em *servidor* literalmente corresponde à saída do `hostname` comando sobre o máquina servidora, ou loop C notícias para sempre na tentativa de entregar o artigo. Discutimos NFS é detalhe em Capítulo 14, *O Network File System*.

Ferramentas de manutenção e tarefas

Apesar da complexidade do C News, a vida de um administrador da notícia pode ser razoavelmente fácil; C News oferece-lhe

uma
grande variedade de ferramentas de manutenção. Algumas delas são destinadas a ser executado regularmente a partir de `cron`, Como `NewsDaily`.
Usando esses scripts reduz muito cuidado diário e necessidades alimentares de sua instalação News C.

Salvo disposição em contrário, esses comandos estão localizados na */ Usr / news / lib / maint*. (Note que você deve se tornar

usuário
notícias antes de chamar esses comandos. Executá-los como um superusuário pode tornar inacessíveis newsfiles crítica Notícias de C).:

`NewsDaily`

O nome já diz: executar isto uma vez por dia. É um script importante que ajuda a manter arquivos de log pequeno, mantendo cópias de cada a partir dos últimos três corridas. Ele também tenta anomalias sentido, como lotes obsoleto
nos lançamentos de entrada e saída de diretórios, para desconhecidos ou newsgroups moderados, etc Resultante mensagens de erro serão enviadas para o newsmaster.

`Newswatch`

Este script deve ser executado regularmente para procurar anomalias no sistema de notícias, uma vez que uma hora ou assim. É em
tenderam a detectar problemas que terá um efeito imediato sobre a operacionalidade do seu sistema de notícias, em

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

que no caso mails um relatório de problemas para o newsmaster. Coisas verificados incluem arquivos de bloqueio vencido que não
são removidos, os lotes de entrada automática, e falta de espaço em disco.

131 Eu não tentaria isso na internet, qualquer um.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`addgroup`

Esse script adiciona um grupo no seu site localmente. A invocação apropriada é:

`addgroup` *groupname* `y | n | m |` *=realgroup*

O segundo argumento tem o mesmo significado que a bandeira na *ativos* arquivo, o que significa que qualquer pessoa

pode enviar para o
grupo (*y*), Que ninguém pode post (*n*), Que é moderado (*m*), Ou que é um alias para outro grupo (*= Realgroup*).
Você também pode querer usar `addgroup` quando os primeiros artigos de um grupo recém-criado chegar mais cedo do que o *newgroup* controle de mensagem que se pretende criar.

`delgroup`

Este script permite que você excluir um grupo local. Invocá-la como:

`delgroup` *groupname*

Você ainda tem que eliminar os artigos que permanecem no diretório de spool do grupo de notícias. Alternativamente,

você
pode deixar para o curso natural dos acontecimentos (ou seja, validade), para torná-los ir embora.

`addmissing`

Este script acrescenta artigos à falta *história* arquivo. Executá-lo quando há artigos que parecem cair
para sempre.

`newsboot`

Este script deve ser executado em tempo de inicialização do sistema. Ele remove todo o fechamento de arquivos que

sobraram quando a notícia processos
foram mortos durante o desligamento, e fecha e executa os lotes que sobraram de conexões de NNTP que
foram encerrados ao desligar o sistema.

`newsrunning`

Este script reside em */ Usr / news / lib / input* e pode ser usado para desativar unbatching de notícias recebidas, para exemplo, durante as horas de trabalho. Você pode desligar unbatching invocando:

```
/ Usr / lib / news / input / newsrunning off
```

Ele é ligado por meio *em* em vez de *fora*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 22 - NNTP eo Daemon nntpd

Network News Transfer Protocol (NNTP) prevê uma abordagem muito diferente para trocar as notícias de C
Notícias e outros servidores de notícias sem suporte nativo NNTP. Ao invés de contar com uma tecnologia de lote como o UUCP
a transferência de artigos de notícias entre as máquinas, permite que os artigos a serem trocadas através de uma rede interativa cone-
ção. NNTP não é um pacote de software específico, mas um padrão de Internet descrito na RFC-977. É baseado em um
conexão orientado a fluxo, geralmente através de TCP, entre um cliente em qualquer lugar da rede e um servidor em um host
que mantém Netnews com armazenamento em disco. A conexão permite que o fluxo de cliente e servidor para negociar de forma interativa
transferência artigo com quase nenhum atraso de resposta, mantendo assim duplicar o número de artigos de baixo. Juntamente com
taxas de transferência da Internet de alta, este acrescenta-se a um transporte de notícias que ultrapassa as redes UUCP original por
distante. Enquanto alguns anos atrás não era incomum para um artigo para levar duas semanas ou mais antes de chegar na
última curva da Usenet, e é hoje muitas vezes menos de dois dias. Na própria internet, é ainda dentro do intervalo de min-
nutos.

Vários comandos permitem aos clientes obter, enviar e publicar artigos. A diferença entre enviar e postagem
é que o último pode envolver artigos com informações de cabeçalho incompletas, que geralmente significa que o usuário tem
acabou de escrever o artigo.[132] recuperação do artigo pode ser usado por clientes de transferência de notícias, bem como locutores. Este
NNTP torna uma excelente ferramenta para facilitar o acesso de notícias para muitos clientes em uma rede local sem passar
através dos contorcionismos que são necessários quando se usa NFS.

NNTP prevê igualmente um papel activo e de forma passiva a transferência de notícias, coloquialmente chamado de "empurrar"

e "pull-
ing. "Pushing é basicamente o mesmo que o protocolo / ihave sendme utilizado por C News (descrito no Capítulo 21, *C Notícias*). O cliente oferece um artigo para o servidor através da `IHAVE msgstr` comando, eo servidor retorna uma
código de resposta que indica se ele já possui o artigo ou se ele quer isso. Se o servidor quiser o artigo, o
cliente envia o artigo, denunciado por um único ponto em uma linha separada.

Pushing notícia tem a desvantagem único que coloca uma carga pesada no sistema do servidor, desde que o sistema tem
para procurar seu banco de dados de histórico para cada artigo.

A técnica oposta está puxando coletiva em que o cliente solicita uma lista de todos os artigos (disponível) de um grupo
que chegaram após uma data especificada. Essa consulta é realizada pela `Newnews` comando. De retornado
lista de identificações de mensagem, o cliente escolhe os artigos que ainda não tem, usando o `ARTIGO` comando para cada
um deles em separado.

Agarrar notícias necessidades controlo apertado pelo servidor durante o qual os grupos e as distribuições que permite que um

cliente solicitar.
Por exemplo, tem que se certificar de que nenhum material confidencial de newsgroups local para o site é enviado para unau-
clientes não autorizadas.

Há também uma série de comandos de conveniência para locutores que lhes permita recuperar o artigo
cabeçalho e corpo separadamente, ou mesmo linhas de cabeçalho único a partir de uma série de artigos. Isso permite que você mantenha todas as notícias sobre um
host central, com todos os usuários na rede (provavelmente local) usando programas clientes NNTP-base para a leitura e
postagem. Esta é uma alternativa para a exportação dos diretórios notícias via NFS, conforme descrito no capítulo 21.

Um problema global do NNTP é que permite que uma pessoa experiente para inserir artigos no fluxo de notícias com
especificação de remetente falso. Isso é chamado *notícias fingindo* ou *spoofing.*[133] Uma extensão NNTP permite exigir
autenticação de usuário para certos comandos, proporcionando certa proteção contra as pessoas abusando de seu
servidor de notícias desta maneira.

Há uma série de pacotes de NNTP. Um dos mais conhecidos é o servidor de NNTP, também conhecido como o
implementação de referência. Originalmente, ela foi escrita por Stan Barber e Phil Lapsley para ilustrar os detalhes de
RFC-977. Tal como acontece com grande parte do bom software disponível hoje, você pode encontrá-lo pré-embalados para o seu dis-Linux
ção, ou você pode obter a fonte e compilá-la. Se você optar por compilar você mesmo, você vai
precisará ser bastante familiarizado com a sua distribuição para garantir que você configurar todos os caminhos de arquivo

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

corretamente.

A `nntpd` pacote tem um servidor, dois clientes para puxar e empurrar, notícias e um `inews` substituição. Eles
viver em um ambiente de Notícias B, mas com um pouco de ajustes, eles serão felizes com o C News, também. Entretanto, se você
planeja usar NNTP para mais de locutores, que oferecem acesso a seu servidor de notícias, a implementação de referência

132 Ao postar um artigo sobre NNTP, o servidor adiciona sempre pelo menos um campo de cabeçalho, `NNTP-Posting-Host:`. O campo de contém hostname do cliente.

133 O mesmo problema existe com o Simple Mail Transfer Protocol (SMTP), embora a maioria dos agentes de transporte de correio agora fornecer mecanismos para impedir a falsificação.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

não é realmente uma opção. Por isso vamos discutir apenas o daemon NNTP contidas no `nntpd` pacote e deixar de fora os programas cliente.

Se você desejar executar um grande site de notícias, você deve olhar para o *Internet News* pacote, ou DCI, que foi escrito por Rich Salz. Ele proporciona tanto NNTP e transporte de notícias UUCP-based. transporte de notícias é definitivamente melhor do que
`nntpd`. Discutimos INN em detalhes no Capítulo 23, *Internet News*.

O protocolo NNTP

Nós mencionamos dois comandos NNTP que são essenciais ao modo como artigos de notícia são empurrados ou puxados entre os servidores.

Agora vamos olhar para estes, no contexto de uma sessão de NNTP real para mostrar como o protocolo é simples. Para os propósitos de nossa ilustração, vamos usar um simples `telnet` cliente para se conectar a um servidor de notícias INN baseado na
Cervejaria chamado Virtual news.vbrew.com. O servidor está executando uma configuração mínima para manter os exemplos curto. Veremos como para completar a configuração deste servidor no capítulo 23. Em nossos testes, vamos ser muito o cuidado de gerar artigos na *lixo* newsgroup apenas, para evitar perturbar ninguém.

Conectando ao servidor de notícias

Conectando ao servidor de notícias é tão simples como abrir uma conexão TCP à porta NNTP. Quando você estiver conectado, você será saudado com uma faixa de boas-vindas. Um dos primeiros comandos que você pode tentar é *Ajuda*. A resposta você começa geralmente depende se o servidor acredita que você é um servidor de NNTP remoto ou uma notícia-leitor, uma vez que existem diferentes conjuntos de comandos necessários. Você pode mudar seu modo de operação usando o `Modo`
comando, veremos que, em um momento:

```
$ nntp news.vbrew.com telnet
Tentando 172.16.1.1 ...
Connected to localhost.
Escape character is'^]'.
200 news.vbrew.com servidor InterNetNews INN 1.7.2 08-Dez-1997 está pronto
Ajuda
100 comandos legais
        AuthInfo
               Ajuda
               ihave
               seleção
               takethis
               lista
               Modo
               xmode
               parar
               cabeça
               stat
               xbatch
               xpath
               xreplic
Para obter mais informações, entre em contato "Usenet" nesta máquina.
.
```

As respostas aos comandos NNTP sempre terminam com um ponto (.) Em uma linha por si só. Os números que você vê na anúncio de saída são *códigos de resposta* e são usados pelo servidor para indicar sucesso ou fracasso de um comando. A códigos de resposta são descritos na RFC-977, vamos falar sobre os mais importantes à medida que avançarmos.

Empurrando um artigo de notícia para um servidor

Nós mencionamos o `IHAVE` comando quando falamos empurrando artigos de notícia em um servidor de notícias. Vamos agora ter um olhar como o `IHAVE` comando realmente funciona:

```
ihave <123456@gw.vk2ktj.ampr.org>
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

De: terry@gw.vk2ktj.ampr.org
Assunto: mensagem de teste enviada com ihave
Grupos de notícias: lixo
Distribuição: o mundo
Caminho: gw.vk2ktj.ampr.org
Data: 26 de abril de 1999
<123456@gw.vk2ktj.ampr.org> Message-ID
Corpo:

Esta é uma mensagem de teste enviada através do NNTP comando IHAVE.

.
235

Todos os comandos NNTP são caso insensitivo, então você pode inseri-los em qualquer maiúsculas ou minúsculas. A `IHAVE` comando tem um argumento obrigatório, sendo a mensagem de identificação do artigo que está sendo empurrado. Cada notícia artigo é atribuída uma identificação única mensagem quando ela é criada. A `IHAVE` comando fornece uma maneira de o NNTP servidor para dizer quais os artigos que tem quando quer empurrar artigos para outro servidor. O servidor de envio emitirá um `IHAVE` comando para cada artigo que deseja enviar. Se o código de resposta do comando gerado pelo recebimento servidor NNTP está na faixa "3xx", o servidor de envio NNTP irá transmitir o artigo completo, incluindo a sua completa cabeçalho, que encerra o artigo com um período em uma linha por si só. Se o código de resposta estava na faixa "4xx", o servidor de recebimento optou por não aceitar este artigo, possivelmente porque ele já tem, ou por causa de alguns proble-blema, como a falta de espaço em disco.

Quando o artigo foi transmitida, o recebimento servir questões outro código de resposta indicando se o transmissão artigo foi bem sucedida.

Mudar para Modo nnrp Reader

Locutores usando seu próprio conjunto de comandos quando se fala de um servidor de notícias. Para ativar esses comandos, o servidor de notícias tem que estar operando em *leitor* modo. A maioria das notícias padrão de servidores para o modo de leitor, a menos que o endereço IP
do hospedeiro se conectando é listado como um par de notícias de encaminhamento. Em qualquer caso, NNTP fornece um comando de forma explícita
alternar para o modo de leitor:

modo leitor

```
200 news.vbrew.com InterNetNews servidor nnrp INN 1.7.2 08-Dez-1997 prontos /
    (Postagem ok).
```

Ajuda

```
100 comandos legais
  Nome de usuário AuthInfo | pass Senha | genéricos <prog> <args>
  artigo [MessageID | Número]
  corpo [MessageID | Número]
  data
  grupo de notícias
  cabeça [MessageID | Número]
  Ajuda
  ihave
  passado
  lista [activa | active.times | newsgroups | distribuições | distrib.pats | /
      overview.fmt |] assinaturas
  listgroup newsgroup
  modo leitor
  newgroups yymmdd hhmmss ["GMT"] [<distributions>]
  newsgroups newnews YYMMDDHHMMSS ["GMT"] [<distributions>]
  próxima
  post
  escravo
  stat [MessageID | Número]
  xgtitle [group_pattern]
  xhdr cabeçalho intervalo [| MessageID]
  Xover intervalo []
  faixa de cabeçalho Xpat | pat MessageID [morepat ...]
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
  MessageID xpath
Relatar problemas para <usenet@vlager.vbrew.com>
.
```

NNTP modo leitor tem um monte de comandos. Muitos destes são projetadas para tornar a vida de um leitor mais fácil. Mencionamos anteriormente que existem comandos que instruem o servidor para enviar a cabeça eo corpo de artigos separadamente. Há também os comandos que lista os grupos disponíveis e artigos, e outros que permitem destacamento, um meios alternativos de envio de notícias para o servidor.

Listagem de Grupos disponíveis

A `lista` comando enumera uma série de diferentes tipos de informação, nomeadamente os grupos apoiados pelo servidor:

grupos de discussão lista

```
215 descrições em forma de "descrição do grupo".
controle                Notícias grupo de servidores internos
lixo                    Notícias grupo de servidores internos
local.general           General material local
local.test              grupo de teste local
.
```

Listagem de grupos do

Active

lista ativa mostra cada grupo apoiou e fornece informações sobre eles. Os dois números em cada linha de a saída é a marca d'água ea maré baixa - menor que seja, o maior artigo numeradas e numerado artigo em cada grupo. O leitor é capaz de formar uma idéia do número de artigos do grupo a partir destes. Vamos falar um pouco mais sobre esses números em um momento. O último campo mostra as opções de saída que controlam se o lançamento é permitido para o grupo, se o grupo é moderado, e se artigos postados são realmente armazenados ou apenas passadas. Esses sinalizadores são descritos em detalhe no Capítulo 23. Um exemplo parece isso:

lista ativa

```
215 Grupos de notícias em forma de "grupo de alto bandeiras baixo".
Y Control 0000000000 0000000001
lixo 0000000003 0000000001 y
alt.test y 0000000000 0000000001
.
```

Publicar um artigo

Mencionamos havia uma diferença entre empurrar um artigo e postar um artigo. Quando você está empurrando um artigo, há um pressuposto implícito de que o artigo já existe, que tem um identificador de mensagem que tem foi exclusivamente atribuído a ela pelo servidor para o qual foi originalmente publicado, e que tem um conjunto completo de cabeçalhos. Ao postar um artigo, você está criando o artigo pela primeira vez e somente os cabeçalhos que você fornecer são aqueles que são significativos a você, como o assunto e newgroups ao qual você está postando o artigo. O servidor de notícias que você postar o artigo sobre irá adicionar todos os outros cabeçalhos para você e para criar um ID da mensagem que ele vai usar ao empurrar o artigo em outros servidores.

Tudo isso significa que um artigo publicado, é ainda mais fácil do que empurrar um. Um exemplo postagem parecido com este:

post

```
340 Ok
De: terry@richard.geek.org.au
Assunto: teste mensagem número 1
Grupos de notícias: lixo
Corpo:

Esta é uma mensagem de teste, por favor, sinta-se livre para ignorá-la.

.
240 Artigo postado
```

Vamos mais duas mensagens como esta para dar aos nossos exemplos que se seguem algum realismo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Listagem de artigos Novos

Quando um leitor conecta pela primeira vez para um novo servidor eo usuário escolhe um grupo de discussão para navegar, o

leitor de notícias
vai querer recuperar uma lista de novos artigos, os postados ou recebidos desde o último login do usuário. A *newnews* comando é usado para esta finalidade. Três argumentos obrigatórios devem ser fornecidos: o nome do grupo ou grupos para consulta, a data de início eo horário de início a partir do qual a lista. A data ea hora são especificadas como cada seis dígitos, com as informações mais importantes em primeiro lugar; *yymmdd* e *hhmmss*, Respectivamente:

newnews lixo 990101 000000
```
230 notícias Nova segue
<7g2o5r $ aa $ 6@news.vbrew.com>
<7g5bhm $ 8f $ 2@news.vbrew.com>
<7g5bk5 $ 8f $ 3@news.vbrew.com>
.
```

Selecionando um grupo em que a operar

Quando o usuário seleciona um grupo de discussão para navegar, o leitor pode dizer ao servidor de notícias que o grupo foi se-selecionada. Isso simplifica a interação entre leitor e servidor de notícias, que suprime a necessidade de constantemente enviar o nome do grupo de notícias com cada comando. A *grupo* comando simplesmente leva o nome do escolhido grupo como um argumento. Muitos comandos a seguir usam o grupo selecionado como padrão, a menos que outra notícia-grupo é especificado explicitamente:

sucata grupo
```
211 3 1 3 sucata
```

A *grupo* comando retorna uma mensagem indicando o número de mensagens ativa, a baixa-mar, a alta marca d'água, eo nome do grupo, respectivamente. Observe que, embora o número de mensagens ativo eo marca d'água são os mesmos, no nosso exemplo, isto não é frequentemente o caso, em um servidor de notícias da ativos, alguns artigos
pode ter expirado ou ter sido excluído, diminuindo o número de mensagens ativas, mas deixando a marca de água de alta intocada.

Listagem de artigos em um grupo

Para lidar com artigos de notícias, o leitor deve saber quais números representam artigos ativo. A *listgroup* comando oferece uma lista dos números artigo activo no grupo atual, ou um grupo explícito se o nome do grupo é prestado:

listgroup lixo
```
211 lista do artigo seguinte
1
2
3
.
```

Recuperando um cabeçalho Apenas artigo

O usuário deve ter alguma informação sobre um artigo antes que ela possa saber se ela deseja ler. Nós mencionado anteriormente que alguns comandos permitem que o cabeçalho eo corpo do artigo a ser transferido separadamente. A *cabeça*
comando é usado para solicitar que o servidor transmite apenas o cabeçalho do artigo especificado para o leitor. Se o usuário não quiser ler este artigo, nós não perdemos tempo e largura de banda da transferência de uma po-cialmente corpo do artigo desnecessariamente grande.

Os artigos podem ser referenciados usando o seu número (a partir do *listgroup* comando) ou identificador de sua mensagem:

cabeça 2
```
221 2 <7g5bhm $ 8f $ 2@news.vbrew.com cabeça>
Caminho: news.vbrew.com sem fins-mail!
De: terry@richard.geek.org.au
Grupos de notícias: lixo
Assunto: mensagem de teste número 2
Data: 27 de abril de 1999 21:51:50 GMT
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
Organização: A cervejaria Virtual
Linhas: 2
<7g5bhm $ 8f $ 2@news.vbrew.com> Message-ID
NNTP-Posting-Host: localhost
X-Server Data: 27 de abril de 1999 21:51:50 GMT
Corpo:
Xref: news.vbrew.com lixo: 2
.
```

Recuperando um corpo apenas o artigo

Se, por outro lado, o usuário decide se quer ler o artigo, o seu leitor precisa de uma forma de solicitar que o corpo da mensagem ser transmitida. A *corpo* comando é usado para esta finalidade. Ele opera da mesma forma e maneira como a *cabeça* comando, exceto que somente o corpo da mensagem é retornada:

corpo 2

```
222 2 <7g5bhm $ 8f $ 2@news.vbrew.com corpo>
Esta é outra mensagem de teste, por favor, sinta-se livre para ignorá-la também.
.
```

Lendo um artigo de um grupo

Embora seja normalmente mais eficiente para transferir em separado os cabeçalhos e corpos de artigos selecionados, existem ocasiões em que estamos melhor transferir o artigo completo. Um bom exemplo disso é em aplicações através do qual pretende transferir todos os artices em um grupo sem qualquer tipo de pré-selecção, como quando nós estiver usando um programa como o cache NNTP `leafnode`.[134]

Naturalmente, NNTP fornece um meio de fazer isso, e não surpreende, ela opera de forma quase idêntica à *cabeça* comando também. A *artigo* comando também aceita um número ou identificação da mensagem como um argumento, mas re-transforma todo o artigo, incluindo seu cabeçalho:

artigo 1 º

```
220 1 <7g2o5r $ aa $ 6@news.vbrew.com> Artigo
Caminho: news.vbrew.com sem fins-mail!
De: terry@richard.geek.org.au
Grupos de notícias: lixo
Assunto: teste mensagem número 1
Data: 26 de abril de 1999 22:08:59 GMT
Organização: A cervejaria Virtual
Linhas: 2
<7g2o5r $ aa $ 6@news.vbrew.com> Message-ID
NNTP-Posting-Host: localhost
X-Server Data: 26 de abril de 1999 22:08:59 GMT
Corpo:
Xref: news.vbrew.com lixo: 1

Esta é uma mensagem de teste, por favor, sinta-se livre para ignorá-la.

.
```

Se você tentar recuperar um artigo desconhecido, o servidor retornará uma mensagem com uma adequada re-codificado código de resposta e talvez uma mensagem de texto legível:

artigo 4 º

```
423 número Bad
```

Nós descrevemos como os mais importantes comandos NNTP são usadas nesta seção. Se você estiver interessado em desen- em desenvolvimento de software que implementa o protocolo NNTP, você deve consultar os documentos pertinentes, RFC, eles pró- vide uma grande quantidade de detalhes que não podíamos incluir aqui.

Vamos agora olhar para NNTP em ação através da nntpd servidor.

---

134 *leafnode* está disponível por FTP anônimo wpxx02.toxi.uni-wuerzburg.de na */ Pub /* diretório.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Instalando o Servidor NNTP

O servidor NNTP (nntpd) Pode ser compilado de duas maneiras, dependendo da carga de espera no sistema de notícias. Não existem versões compiladas disponíveis, por causa de alguns padrões do site-specific que são codificados na executável. Toda a configuração é feita através de macros definidas *comum / conf.h*.

nntpd pode ser configurado como um servidor autônomo que é iniciado no tempo de inicialização do sistema a partir de um `rc` arquivo, ou uma
daemon gerido pela `inetd`. Neste último caso, você tem que ter a seguinte entrada no */ Etc / inetd.conf*:

```
nntp    stream  tcp nowait      notícia / Usr / etc /        nntpd
                                s       in.nntpd
```

A *inetd.conf* sintaxe é descrita em detalhes no Capítulo 12, *Rede Características importantes*. Se você configurar `nntpd` como autônomo, certifique-se que qualquer linha, na `inetd.conf` é comentada. Em ambos os casos, você tem que fazer se a seguinte linha aparece na */ Etc / services*:

```
nntp    119/tcp   readnews untp    # Network News Transfer Protocol
```

Para armazenar temporariamente todos os artigos recebidos, `nntpd` também precisa de um *. Tmp* diretório em seu spool de notícias. Você deve
criá-lo usando os seguintes comandos:

```
#  mkdir / var / spool / news / .tmp
#  chown news.news var / spool / news .tmp /
```

Restringindo o acesso de NNTP

O acesso aos recursos NNTP é governado pelo arquivo *nntp_access* em */ Notícias / etc*. As linhas neste arquivo descrever o acesso
direitos concedidos aos exércitos estrangeiros. Cada linha tem o seguinte formato:

site `leia | xfer | ambos  post | não  [!`*exceptgroups*`] | não`

Se um cliente se conecta à porta NNTP, nntpd tentativas de obter o nome do host de domínio totalmente qualificado do seu endereço IP usando inversa. hostname do cliente eo endereço IP são confrontados com os *site* campo de cada entrada na ordem em que aparecem no arquivo. Os jogos podem ser parciais ou exatas. Se uma entrada partidas exatamente, ele se aplica, se o jogo for parcial, só se aplica se não houver nenhum outro jogo seguinte, que é pelo menos tão bom. *site* podem ser especificados em uma das seguintes formas:

Hostname

> Este é um nome de domínio totalmente qualificado de um hospedeiro. Se isso corresponde hostname canônica do cliente, literalmente,
> a entrada se aplica, e todas as entradas seguintes são ignoradas.

endereço IP

> Este é um endereço IP na notação "dotted quad. Se o endereço IP do cliente corresponde a esta, a entrada se aplica, e todas as entradas seguintes são ignoradas.

Nome de domínio

> Este é um nome de domínio especificado como *Domínio* *.. Se hostname do cliente corresponde ao nome de domínio, o entrada encontrados.

O nome da rede

> Este é o nome de uma rede, conforme especificado no */ Etc / networks*. Se o número da rede do anúncio do cliente IP vestido corresponde ao número de rede associado ao nome da rede, a entrada encontrados.

Default

> A seqüência de `padrão` corresponde a qualquer cliente.

Entradas com uma especificação de local mais gerais devem ser especificados anteriormente, porque as correspondências serão substituídos
pela tarde, os jogos mais exato.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

O segundo e terceiro campos descrever os direitos de acesso concedidos ao cliente. Os detalhes do segundo campo a permissões para recuperar notícias puxando (*leia*), E transmitir notícias, empurrando (*xfer*). Um valor de *ambos* permite a ambos; *não* nega o acesso completamente. As bolsas terceiro campo o cliente o direito de publicar artigos, por exemplo, entregar artigos com informações de cabeçalho completo, que é completada pelo software notícia. Se o segundo campo contém *não*, O terceiro campo é ignorado.

O quarto campo é opcional e contém uma lista separada por vírgulas de grupos aos quais o cliente é negado o acesso.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Esta é uma amostra *nntp_access* arquivo:

```
#
# Por padrão, qualquer pessoa pode transferir notícia, mas não sabem ler
ou postar
padrão                  xfer            não
#
public.vbrew.com # oferece acesso via modem. Nós permitimos
#-Los a ler e enviar mensagens para qualquer mas o local .* grupos
public.vbrew.com        leia            post    ! Local
#
# Todos os outros hosts na cervejaria pode ler e postar
*. Vbrew.com            leia            post
```

NNTP Autorização

A `nntpd` daemon prevê um regime de autorização simples. Se você tirar qualquer um dos tokens de acesso na *nntp_access* arquivo, `nntpd` requer autorização do cliente para a respectiva operação. Por exemplo, quando especificando uma permissão de *Xfer* ou *XFER*, (Em oposição a *xfer*), `nntpd` não vai deixar os artigos cliente de transferência de
seu site a menos que ele passa autorização.

O processo de autorização é implementada por meio de um comando NNTP novo nomeado `AuthInfo`. Usando este comando, o cliente envia um username e uma senha para o servidor NNTP. `nntpd` valida-los por meio de chequeção contra os */ Etc / passwd* banco de dados e verifica se o usuário pertence ao *nntp* grupo.

A implementação atual de autorização NNTP é apenas experimental e portanto não foi implementado
muito portável. O resultado disso é que ele só funciona com bancos de dados de senha simples de estilo; senhas de sombra são não reconhecido. Se você está compilando o código e ter o pacote PAM instalado, a verificação da senha é
bastante simples de mudar.

Interação com nntpd C News

Quando `nntpd` recebe um artigo, ele tem que entregar para o subsistema de notícias. Dependendo se foi re-
percebida como resultado de um `IHAVE` ou `POST` comando, o artigo é entregue ao `rnews` ou `inews`, Respectivamente. Em vez de invocar `rnews`, Você também pode configurá-lo (em tempo de compilação), ao lote de artigos recebidos e mover os lotes resultantes de */ Var / spool / news / in.coming*, Onde são deixados para `relaynews` para pegá-los na
o funcionamento da fila seguinte.

`nntpd` tem que ter acesso ao *história* arquivo para ser capaz de executar corretamente o protocolo / ihave sendme. Em com-
tempo de pilha, você tem que fazer se o caminho para que o arquivo está configurado corretamente. Se você usar C News, certifique-se que C News
e `nntpd` acordo sobre o formato do seu arquivo histórico. C usa Notícias *dbm* funções hash para acessá-lo, no entanto, há um grande número de implementações diferentes e um pouco incompatível do *dbm* biblioteca. Se News C
tem sido associada com um diferente *dbm* biblioteca que você tem no seu padrão */ibc*, Você tem que ligar `nntpd` com esta biblioteca, também.

`nntpd` e C desacordo notícias às vezes produz mensagens de erro no log do sistema que `nntpd` não pode abri-lo corretamente, ou você poderá ver artigos duplicados sendo recebidos via NNTP. Um bom teste de avaria transferência notícia é pegar um artigo da sua área de spool, telnet para o nntp porto, e oferecê-lo a `nntpd` como mostrado no exemplo seguinte. Claro, você tem que substituir *msg @ id* com a identificação da mensagem do artigo que você quer alimentar
para `nntpd`:

```
$ nntp telnet localhost
Trying 127.0.0.1 ...
Conectado ao localhost
Caracteres de escape é '] ^'.
201 vstout NNTP [auth] servidor 1.5.11t versão (16 de Novembro de 1991) no pronto
Dom 06 de fevereiro 16:02:32 1194 (sem postagem)
IHAVE msg @ id435 Got it.
QUIT
```

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Essa conversa mostra `nntpd`"A reação adequada, a mensagem `Entendi` diz-lhe que ele já tem este artigo.
Se você receber uma mensagem de `335 Ok` em vez disso, a pesquisa no arquivo histórico falhou por algum motivo. Encerrar o conversa com Ctrl-D. Você pode verificar o que deu errado, verificando o log do sistema; `nntpd` registra todos os tipos de mensagens para o *daemon* facilidade de `syslog`. Um incompatíveis *dbm* biblioteca geralmente se manifesta em uma mensagem reclamando que *dbminit* falhou.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 23 - Notícias da Internet

A Internet daemon News (DCI) é sem dúvida o mais popular servidor Netnews em uso hoje. DCI é extremamente flexível e adequado para todos, mas os sites de notícias menor.[135] escalas DCI bem e é adequado para servidor de notícias grande configurações.

O servidor INN dispõe de um número de componentes, cada um com seus próprios arquivos de configuração que iremos discutir por sua vez. Configuração do DCI pode ser um pouco envolvidos, mas vamos descrever cada uma das etapas neste capítulo e armá-lo com informações suficientes para fazer o sentido das páginas de manual e documentação INN e construir configurações para praticamente qualquer aplicação.

Alguns DCI Internals

programa DCI do núcleo é o `innd` daemon. `innd`'S é tarefa para lidar com todos os artigos recebidos, armazená-los localmente, e passá-las a qualquer newsfeeds saída, se necessário. É iniciado na inicialização e funciona continuamente como um fundo processo. Correndo como um daemon melhora o desempenho, porque tem de ler o seu estatuto de arquivos apenas uma vez quando se inicia. Dependendo do volume do seu feed de notícias, alguns arquivos, como *história* (Que contêm uma lista de todos os artigos recentemente processado) pode variar de poucos megabytes a dezenas de megabytes.

Outra característica importante do DCI é que há sempre apenas uma instância de `innd` correndo a qualquer momento. Esta é também muito benéfico para o desempenho, pois o daemon pode processar todos os artigos sem ter que se preocupar sincronizar seus estados internos com outras cópias do `innd` remexendo o spool de notícias ao mesmo tempo.
No entanto, esta escolha afeta o design geral do sistema de notícias. Porque é tão importante que a entrada notícia é processada o mais rapidamente possível, é inaceitável que o servidor seja amarrado com tarefas tão mundanas como servindo locutores acessar o spool de notícias via NNTP, ou newsbatches descomprimir chegam via UUCP.
Portanto, essas tarefas foram quebradas do servidor principal e aplicado em programas de apoio separado.
Figura 23.1 attemPontos para ilustrar as relações entre `innd`, As outras tarefas locais e servidores remotos de notícias e locutores.

Hoje, NNTP é o meio mais comum de transporte de artigos de notícias ao redor, e `innd` não diretamente sup-
nada porto mais. Isso significa que `innd` escuta em um soquete TCP (porta 119) para conexões e aceita notícia artigos usando o protocolo "ihave".

Artigos que chegam de outros transportes que NNTP são suportados indirectamente, por ter um outro processo de aceitar a artigos e encaminhá-los para `innd` via NNTP. Newsbatches entrando em um link de UUCP, por exemplo, são tradicionalmente tratada pelo `rnews` programa. DCI's `rnews` descompacta o lote, se necessário, ea quebra em artigos individuais, mas, em seguida, oferece-lhes a `innd` um por um.

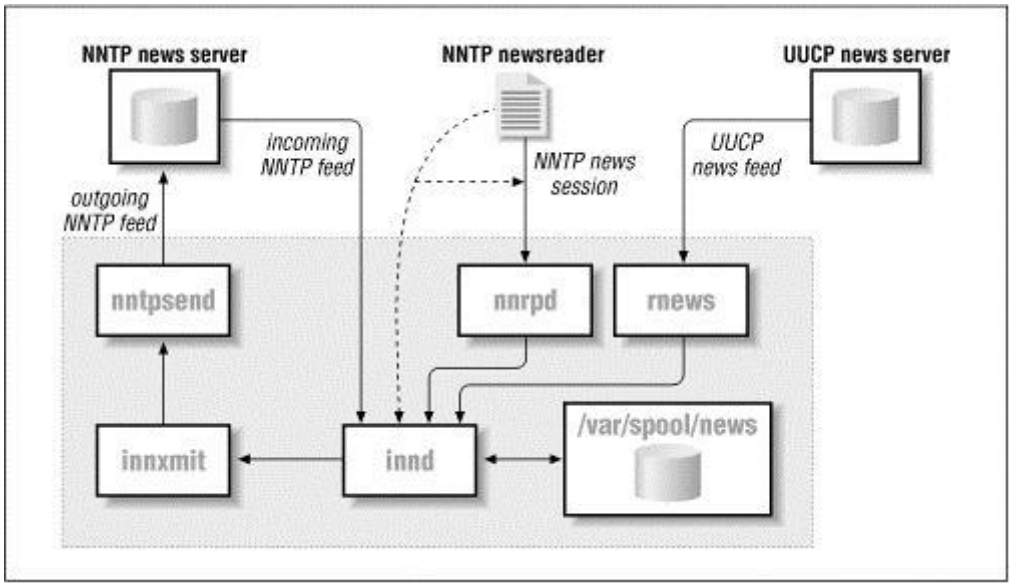
Newsreaders pode entregar a notícia quando um usuário envia um artigo. Desde o tratamento de locutores merece atenção especial
atenção, vamos voltar a este um pouco mais tarde.

---

135 Muito sites de notícias de pequeno porte devem considerar um programa de cache de um servidor NNTP como `leafnode`, Que está disponível em http://wpxx02.toxi.uni-wuerzburg.de/~krasel/leafnode.html.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Figura 23.1: arquitetura DCI (simplificado para maior clareza)



Ao receber um artigo, `innd` primeiro olha o seu ID de mensagem no *história* arquivo. Os artigos duplicados são descartados e, opcionalmente, as ocorrências são registradas. O mesmo vale para os artigos que são demasiado velhos ou falta alguns necessários
campo de cabeçalho, tais como `Assunto:`.[136] Se `innd` considera que o artigo é aceitável, ele olha para o `Grupos de notícias:`
linha de cabeçalho para descobrir o que os grupos tem sido colocada. Se um ou mais destes grupos são encontrados no *ativos* arquivo, o artigo está arquivado no disco. Caso contrário, ele é apresentado para o lixo especiais para grupos.

artigos individuais são mantidas abaixo */ Var / spool / news*, Também chamado de *spool de notícias*. Cada grupo tem um

separado
diretório, em que cada artigo é armazenado em um arquivo separado. Os nomes de arquivo são números consecutivos, de modo que um
artigo na comp.risks podem ser apresentados como *comp/risks/217*, Por exemplo. Quando `innd` acha que o diretório que quer armazenar o artigo em não existir, ele cria automaticamente.

Além de armazenar artigos localmente, você também pode querer passá-los para saída feeds. Esta é regida pelo *newsfeeds* arquivo que lista todos os locais a jusante, juntamente com os grupos de notícias que deve ser consumido por eles.

Assim como `innd`Está recebendo fim, a transformação de notícias de saída é tratada por uma única interface, também. Em vez

de
fazendo todos os transportadores específicos em si, `innd` depende de vários backends para gerenciar a transmissão de artigos para outros servidores de notícias. instalações de saída são coletivamente dublado *canais*. Dependendo de sua finalidade, uma
canal pode ter diferentes atributos que determinam a informação exatamente o que `innd` passa para ele.

Para uma alimentação NNTP saída, por exemplo, `innd` talvez o garfo `innxmit` programa no arranque, e, para cada artigo que deve ser enviado através de que se alimentam, passar sua mensagem de identificação, o tamanho eo nome do arquivo para `innxmit`É a entrada padrão.
Para uma alimentação UUCP saída, por outro lado, pode escrever o tamanho do artigo e nome do arquivo para um arquivo de log especiais,
que é a cabeça por um processo diferente, em intervalos regulares, a fim de criar lotes e filas-los para o UUCP subsistema.

Além destes dois exemplos, existem outros tipos de canais que não são estritamente saída feeds. Estes são utilizados, ~~por exemplo, quando arquivar news~~groups determinados, ou ao gerar informações gerais. Resumo infor-
ção destina-se a ajudar locutores artigos discussão mais eficientemente. locutores estilo antigo tinha de verificar todos os artículos, separadamente, a fim de obter as informações de cabeçalho necessários para enfiar. Isto colocaria um imenso tensão sobre a máquina do servidor, especialmente quando se utiliza NNTP, além disso, era muito lento.[137] Tele Resumo mecanismo alivia este problema prerecording todos os cabeçalhos relevantes em um arquivo separado (chamado . *Resumo*) Para cada newsgroup. Esta informação pode então ser captado por leitores de notícias tanto por lê-lo directamente a partir do diretório de spool, ou usando o `XOVER` comando quando conectado via NNTP. INN tem a `innd` feed daemon

PDF Creator -- PDF4Free v2.0 http://www.pdf4free.com

todos os artigos para o `overchan` comando, que é anexado ao daemon através de um canal. Vamos ver como isso é feito quando discutimos configurar feeds de notícias mais tarde.

136 Isto é indicado pela *Data:* campo de cabeçalho, o limite é geralmente duas semanas.

137 Threading 1.000 artigos quando se fala de um servidor carregado poderia facilmente levar cerca de cinco minutos, que só os mais dedicados da Usenet viciado consideraria aceitável.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Locutores e DCI

Newsreaders rodando na mesma máquina que o servidor (ou de ter montado o spool do servidor de notícias através do NFS) capaz de ler artigos do carretel diretamente. Para publicar um artigo composto pelo usuário, eles invocam a `inews` programa, que acrescenta os campos de cabeçalho que estão faltando e os encaminha para o daemon via NNTP.

Alternativamente, locutores pode acessar o servidor remotamente através de NNTP. Este tipo de conexão é feita dimuito variável de notícias NNTP baseado em alimentos, para evitar prender o daemon. Sempre que um leitor se conecta à servidor NNTP, `innd` garfos de um programa separado chamado `nnrpd`, Que trata da sessão, enquanto `innd` retorna ao as coisas mais importantes (receber a notícia recebida, por exemplo).[138] Você pode estar se perguntando como o `innd` processo pode distinguir entre um feed de notícias de entrada e um leitor de ligação. A resposta é muito simplo: o protocolo NNTP requer que um problema newsreader NNTP baseado em um `modo leitor` comando após coninterligando-se ao servidor, quando este comando é recebido, o servidor começa a `nnrpd` processo, passa a conexão para ele, e retorna à escuta para conexões a partir de outro servidor de notícias. Costumava haver pelo menos um baseado em DOS
leitor que não foi configurado para fazer isso e, portanto, falhou miseravelmente quando se fala de INN, porque `innd` se não reconhecer qualquer um dos comandos usados para ler a notícia, se não sabe a ligação é de uma leitor de notícias.

Vamos falar um pouco mais sobre o acesso ao leitor INN em "Controlando Newsreader de acesso", mais tarde, no capítulo.

Instalando DCI

Antes de mergulhar de configuração DCI, vamos falar sobre a sua instalação. Leia esta seção, mesmo que você tenha instalado DCI de uma das várias distribuições Linux, que contém algumas dicas sobre segurança e compatibilidade.

distribuições Linux incluído Verson INN-1.4sec por algum tempo. Infelizmente, esta versão tinha dois sutil problemas de segurança. Versões modernas não têm esses problemas ea maioria das distribuições incluem um pré-compilado Binária Linux do DCI Versão 2 ou posterior.

Se preferir, você pode construir INN-se. Você pode obter a fonte de *ftp.isc.org* na */ Pousada / ISC /* diretório. Construindo DCI requer que você edite um arquivo de configuração que informa DCI alguns detalhes sobre seu sistema operacional,
e alguns recursos podem exigir modificações menores para a própria fonte.

Compilar o pacote em si é bastante simples: há um script chamado `CONSTRUIR` que irá guiá-lo através do proSEE. A fonte também contém uma extensa documentação sobre como instalar e configurar o DCI.

Depois de instalar todos os binários, alguns ajustes manuais podem ser obrigados a conciliar DCI com outros aplicativos que queiram acessar suas `rnews` ou `inews` programas. UUCP, por exemplo, espera encontrar o `rnews` programa em */ Usr / bin* ou */ Bin*, Enquanto DCI instala-lo em */ Usr / lib / bin* por padrão. Certifique-se */ Usr / bin / lib /* está no padrão
caminho de pesquisa, ou que não são links simbólicos apontando para a localização real do `rnews` e `inews` comandos.

Configurando DCI: A configuração básica

Um dos maiores obstáculos iniciantes podem enfrentar é que o DCI requer uma configuração de rede de trabalho para a função

propErly, mesmo quando rodando em um host autônomo. Portanto, é essencial que o seu kernel suporta TCP / IP-rede de trabalho durante a execução DCI, e que você tenha criado a interface de loopback como explicado no capítulo 5, *Configuração de rede TCP / IP*.

Em seguida, você tem que ter certeza de que `innd` é iniciado no tempo de boot. O padrão DCI instalação fornece um arquivo de

script

chamada *boot* na */ Notícias / etc /* diretório. Se a sua distribuição usa o SystemV estilo `init` pacote, tudo que você precisa fazer é criar um link simbólico a partir do seu */ Etc / pousada / init.d* arquivo apontando para */ Notícias / etc / boot*. Para outros sabores de `init`,
você tem que ter certeza */ Notícias / etc / boot* é executado a partir de um de seus *rc* scripts. Desde DCI requer rede

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

suporte, o script de inicialização deve ser executado *depois* as interfaces de rede estão configurados.

138 O nome, aparentemente, representa NetNews Ler & Daemon Post.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Arquivos de configuração do DCI

Uma vez concluída as tarefas gerais, agora você pode voltar para a parte realmente interessante da DCI: sua configuração arquivos. Todos esses arquivos residem em */ Notícias / etc*. Algumas alterações nos arquivos de configurações foram introduzidas na versão 2, e
é a versão 2 que descrevemos aqui. Se você estiver executando uma versão mais antiga, você deve encontrar este capítulo útil para orientar
você em atualizar sua configuração. Durante as próximas seções, vamos discuti-los um a um, a construção de configuração da Cervejaria Virtual como um exemplo.

Se você quiser saber mais sobre as características dos arquivos de configuração individual, você também pode consultar o

manual
páginas, a distribuição DCI contém páginas do manual individuais para cada um deles.

Global Parâmetros

Há uma série de parâmetros DCI, que são globais por natureza, que sejam relevantes para todos os grupos de discussão

realizados.

O arquivo inn.conf

DCI arquivo de configuração principal é *inn.conf*. Entre outras coisas, determina o nome pelo qual sua máquina está conhecido na Usenet. A versão 2 do DCI permite que um número desconcertante de parâmetros que devem ser configurados neste arquivo. Fortu-
Infelizmente, a maioria dos parâmetros têm valores padrão que são razoáveis para a maioria dos sites. A *inn.conf (5)* Detalhes do arquivo de todos
os parâmetros, e você deve lê-lo com cuidado se você tiver quaisquer problemas.

Um exemplo simples *inn.conf* pode parecer:

```
inn.conf exemplo # para a Cervejaria Virtual
servidor:        vlager.vbrew.com
domínio:         vbrew.com
fromhost:        vbrew.com
pathhost:        news.vbrew.com
organização:     A Cervejaria Virtual
MTA:             / Usr / sbin / sendmail-oi% s
moderatormailer: s@uunet.uu.net%
#
# Caminhos para INN componentes e arquivos.
#
pathnews:               / Usr / lib / news
pathbin:                / Usr / news / lib / bin
pathfilter:             / Usr / lib / news / bin / filtro
pathcontrol:            / Usr / lib / news / bin / controle
pathdb:                 / Var / lib / news
pathetc:                / Notícias / etc
pathrun:                / Var / run / notícias
pathlog:                / Var / log / news
pathhttp:               / Var / log / news
pathtmp:                / Var / tmp
pathspool:              / Var / spool / news
patharticles:           / Var / spool / notícias / artigos
pathoverview:           / Var / spool / news / overview
pathoutgoing:           / Var / spool / news / saída
pathincoming:           / Var / spool / news / incoming
patharchive:            / Var / spool / news / Arquivo
pathuniover:            / Var / spool / news / uniover
overviewname:           . Resumo
```

A primeira linha diz os programas `rnews` e `inews` qual host para manter contato quando entregar artigos. Essa entrada é absolutamente crucial, para passar artigos `innd`, Eles têm de estabelecer uma conexão com o servidor NNTP.

A *domínio* palavra-chave deve especificar a parte do domínio do nome do host de domínio totalmente qualificado. Um casal de

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

programas deve procurar o seu host totalmente qualificado nome de domínio, se o seu resolvedor retorna a biblioteca não qualificados
hostname somente, o nome dado no *domínio* atributo é pregado nela. Não é um problema para configurá-lo, quer forma, por isso é melhor para definir *domínio*.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A próxima linha define o hostname `inews` vai usar ao adicionar um *De:* linha de artigos publicados pelo local usuários. A maioria dos locutores usar o *De:* campo ao redigir uma mensagem de email ao autor de um artigo. Se omitir este campo, ele será o padrão para o seu host de notícias totalmente qualificados nomes de domínio. Este é sempre o melhor ot
escolha. Você pode, por exemplo, notícias e correio tratado por dois diferentes hospedeiros. Neste caso, você fornecer o nome de domínio totalmente qualificado do seu host de correio após a *fromhost* declaração.

A *pathhost* linha define o nome do host DCI é a de adicionar à `Caminho:` campo de cabeçalho sempre que recebe um artigo. Na maioria dos casos, você vai querer usar o nome de domínio totalmente qualificado do seu servidor de notícias, você pode omitir esta
campo desde que é o padrão. Ocasionalmente, você pode querer usar um nome genérico, como news.vbrew.com, Quando servindo um grande domínio. Isso permite que você para mover o sistema de notícias facilmente a um host diferente, você deve escolher em algum momento.

A próxima linha contém o *organização* palavra-chave. Esta declaração permite-lhe configurar o texto `inews` vai posto no `Organização:` linha de artigos publicados por seus usuários locais. Formalmente, você colocaria uma descrição da sua organização ou nome da sua organização na íntegra aqui. Se não quiser ser tão formal, é moda para organizações com um senso de humor para exibi-lo aqui.

A *organização* palavra-chave é obrigatório e especifica o caminho do agente de transporte de correio que serão utilizados para enviar mensagens moderador. `% S` é substituído pelo endereço de e-mail do moderador.

A *moderatormailer* entrada define um endereço padrão usado quando um usuário tenta postar um newsgroup moderado. A lista de endereços de moderador para cada newsgroup é normalmente mantida em um arquivo separado, mas terá um duro tempo manter o controle de todos eles. A *moderatormailer* entrada é, portanto, consultada como um último recurso, se ele for demultado, `inews` irá substituir o `% S` string com o (pouco transformada) newsgroup nome e enviar toda a artigo para este endereço. Por exemplo, ao postar soc.feminism, o artigo é enviado para *soc-feminism@uunet.uu.net*, Dada a configuração acima. No UUNET, deve haver um alias de correio instalada para cada uma dessas apresentações endereços que encaminha automaticamente todas as mensagens para o moderador adequado.

Por fim, cada uma das entradas restantes especifica a localização do componente ou algum arquivo executável que pertencem a DCI. Se você instalou o DCI de um pacote, estes caminhos devem ter sido configurado para você. Se você instalação de origem, você vai precisar garantir que reflectem onde você instalou o DCI.

Configurando Grupos de notícias

O administrador de notícias sobre um sistema é capaz de controlar quais usuários têm acesso a grupos de notícias. INN oferece duas
arquivos de configuração que permitem ao administrador decidir qual newsgroups para apoiar e fornecer descrições para eles.

Os arquivos ativos e newsgroups

A *ativos* e *newsgroups* arquivos são utilizados para armazenar e descrever os grupos de notícias hospedados por este servidor de notícias. Eles
lista de newsgroups que estamos interessados em receber e servir de artigos para, e informações administrativas sobre eles. Esses arquivos são encontrados no */ Var / news / lib /* diretório.

A *ativos* arquivo determina quais newsgroups este servidor suporta. Sua sintaxe é simples. Cada linha da *ativos* arquivo tem quatro campos delimitados por espaço em branco:

```
nome bandeiras lomark himark
```

A *nome* campo é o nome do newsgroup. A *himark* campo é o maior número que foi usado para um artigo em que o grupo de notícias. A *lomark* campo é o menor número de ativos em uso no newsgroup. Para ilustrar como isso funciona, considere os seguintes cenários. Imagine que temos uma recém-criado grupo de notícias: *himark* e *lowmark* são ambos 0, porque não existem artigos. Se post 5 artigos, eles serão numerados de 1 a 5. *himark* será agora igual a 5, o maior artigo, numerados e *lowmark* será igual a 1, o menor artigo ativo. Se o artigo 5 º é cancelado, não haverá mudança; *himark* permanecerá em 5 a assegurar que este número não é realocado e *lowmark* permanecerá em 1, o menor artigo ativo. Se, agora, cancelar artigo 1 º, *himark* permanecerá unmudou, mas *lowmark* será agora igual a 2, porque um não está mais ativo. Se agora postar um novo artigo, será número atribuído 6, portanto, *himark* será agora igual a 6. Artigo 5 º tem sido usado, por isso não vamos transferir isso. *baixa marca* mantém-se em 2. Este mecanismo nos permite atribuir números de artigo exclusivo para novos artigos e

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

calcular aproximadamente quantos artigos existem ativos do grupo: *himark-lowmark*.

O campo pode conter um dos seguintes procedimentos:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

y

Postagem diretamente a este servidor de notícias é permitida.

n

Postagem diretamente a este servidor de notícias não é permitida. Isso impede que locutores de postar diretamente para este servidor de notícias. Novos artigos só podem ser recebidas de outros servidores de notícias.

m

O grupo é moderado. Qualquer artigos postados neste newsgroup são encaminhados para o newsgroup-modera tor, para aprovação antes de entrarem no grupo de notícias. A maioria dos grupos são moderado.

j

Os artigos deste grupo não são mantidos, mas apenas transmitido. Isso faz com que o servidor de notícias para aceitar o artigo,
mas tudo o que vai fazer com ele é passar para o "up-stream" servidores de notícias. Não vai fazer os artigos disponíveis
x os locutores de leitura a partir deste servidor.

Os artigos não podem ser enviadas para este grupo de notícias. A única maneira que os artigos de notícias são entregues para o servidor
está alimentando-os de um outro servidor de notícias. Locutores não podem directamente escrever artigos para este servidor.

=*foo.bar*

Os artigos são apresentados localmente no foo.bar ``"grupo.

Em nossa configuração de servidor simples, vamos realizar um pequeno número de grupos de discussão, para que os nossos */ Var / news / lib / ativo* arquivo
algo parecido com:

```
Y Control 0000000000 0000000001
lixo 0000000000 0000000001 y
rec.crafts.brewing 0000000000 0000000001 y
rec.crafts.brewing.ales 0000000000 0000000001 y
rec.crafts.brewing.badtaste 0000000000 0000000001 y
rec.crafts.brewing.brandy 0000000000 0000000001 y
rec.crafts.brewing.champagne 0000000000 0000000001 y
rec.crafts.brewing.private 0000000000 0000000001 y
```

A *himark* e *lomark* números neste exemplo são aqueles que você usaria ao criar novos grupos de discussão. A *himark* e *lomark* números parecem bastante diferentes de um newsgroup que atua há algum tempo.

A *newsgroups* arquivo é ainda mais simples. Ele fornece uma linha de descrições de grupos de notícias. Alguns leitores são capazes
para ler e apresentar esta informação para um usuário para ajudá-los a decidir se querem inscrever.

O formato do *newsgroups* arquivo é simplesmente:

```
Nome Descrição
```

A *nome* campo é o nome de um newsgroup, e <*descrição* é uma descrição única linha do que de notícias.

Queremos descrever os grupos de notícias que o nosso servidor suporta, por isso vamos construir o nosso *newsgroups* arquivo como segue:

```
rec.crafts.brewing.ales         Cerveja caseira Ales e Lagers
rec.crafts.brewing.badtaste     Cerveja caseira falta cervejas degustação
rec.crafts.brewing.brandy       Home cerveja sua própria Brandy
rec.crafts.brewing.champagne    Home amadurecer o seu próprio champanhe
rec.crafts.brewing.private      O Virtual casa Cervejaria grupo cervejeiras
```

Configurando Newsfeeds

INN oferece ao administrador a notícia capacidade de controlar quais grupos de notícias são encaminhadas para outras notícias servidores e como eles serão encaminhados. O método mais comum utiliza o protocolo NNTP descrito anteriormente, INN, mas também permite newsfeeds através de outros protocolos, tais como UUCP.

O arquivo newsfeeds

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A *newsfeeds* arquivo determina onde artigos de notícia será enviada. Ele normalmente reside no */ Notícias / etc /* diretório.

O formato do *newsfeeds* é um pouco complicado à primeira vista. Vamos descrever o layout geral aqui, e os *notícias feeds (5)* página de manual descreve o que deixamos de lado. O formato é o seguinte:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

```
# Newsfeeds formato de arquivo
site: padrão: Bandeiras: param
site2: pattern2 \
        : Flags2: param2
```

Cada um feed de notícias para um site é descrito por uma única linha, ou podem ser divididas em várias linhas usando o \ contição personagem. A: Os caracteres delimitar os campos em cada linha. O caractere # no início de uma linha de marcas que a linha como um comentário.

A *site* nomes de campo no sítio a que esta descrição refere-alimentação. O nome do site pode ser codificado como você quiser e não precisa ser o nome do domínio do site. O nome do site será utilizado mais tarde e irá se referir a uma entrada em um tabela que fornece o nome da máquina para o `innxmit` programa que transmite as notícias de NNTP para o re-servidor remoto. Você pode ter várias entradas para cada site, cada item será tratado individualmente.

A *padrão* campo especifica quais os grupos de notícias devem ser enviados para este site. O padrão é enviar todos os grupos,

assim se

que é o que você quer, basta fazer este campo vazio. Este campo é normalmente uma lista delimitada por vírgulas de padrões correspondência expressões. O personagem * Combina com zero ou mais de qualquer personagem, o. personagem não tem sig-especial

significância, o! personagem (se usado no início de uma expressão) executa um NOT lógico, eo caráter @ no o início de um nome de newsgroup significa "Não encaminhar todos os artigos que são publicados ou crossposted a este grupo." A lista é lido e analisado da esquerda para a direita, então você deve se assegurar que você coloca as regras mais específicas primeiro.
O padrão:

```
* Rec.crafts.brewing,! Rec.crafts.brewing.poison, @ rec.crafts.brewing.private
```

mandaria todos os *rec.crafts.brewing* hierarquia de notícias *exceto* o *rec.crafts.brewing.poison*. Ele não iria alimentar quaisquer artigos que eram publicados ou cruzados ao *rec.crafts.brewing.private* newsgroup, esses artigos ser preso e está disponível apenas para aquelas pessoas que usam esse servidor. Se você inverteu os dois primeiros modelos, o primeiro padrão seria substituído pelo segundo e você acabaria por alimentar artigos para o *rec.crafts.brewing.poison* newsgroup. O mesmo é verdade para os padrões de primeiro e último, você deve sempre colocar o padrões mais específicos antes de quaisquer padrões menos específico para que eles entrem em vigor.

bandeiras controles e impõe restrições na alimentação de notícias a este site. A *bandeiras* campo é delimitado por uma vírgula lista pode conter qualquer um dos itens da lista a seguir, delimitado pelos comandos:

<*tamanho*

O artigo deve ser inferior a bytes de tamanho.

A*itens*

verifica artigo. *itens* pode ser um ou mais dos `d` (Deve ter o cabeçalho de Distribuição) ou `p` (Não se verificar para site no cabeçalho de caminho).

B*alta*/*baixa*

Interno tamanho do buffer antes de escrever para a saída.

H[*contagem*]

O artigo deve ter menos de *contagem* lúpulo, o padrão é 1.

I*tamanho*

Tamanho do buffer interno (para uma alimentação de arquivo).

M*padrão*

Só moderado grupos que correspondem ao padrão.

N*padrão*

Só unmoderated grupos que correspondem ao padrão.

S*tamanho*

Iniciar spooling se mais do que ficar na fila bytes de tamanho.

T*tipo*

Feed tipos: `f` (Arquivo) `m` (Funil, o *param* nomes de campo na entrada que os artigos serão canalizados para), `p` (Tubulação para o programa), `c` (Enviar para o canal do stdin *param* subprocesso de campo), e `x` (Como C, mas lida com-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

mandos em stdin).

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Witens

O que escrever: `b` (Bytesize artigo), `f` (Caminho completo), `g` (Primeiro newsgroup), `m` (Message ID), `n` (Caminho relativo),
`s` (Artigo site alimentados isso), `t` (Hora de recepção), `*` (Nomes de funil feed-ins ou todos os sites que recebem do artigo), `N`
(Cabeçalho newsgroups), `D` (Cabeçalho de distribuição), `H` (Todos os cabeçalhos), `O` (Resumo de dados), e `R` (Replicação
de dados).

A `param` campo tem codificação especial que é dependente do tipo de alimentação. Na configuração mais comum,
é onde você especifica o nome do arquivo de saída para o qual você vai escrever o feed de saída. Em outras palavras, configurações pode deixá-lo fora. Em ainda outras configurações que assume diferentes significados. Se você quiser fazer alguma coisa incomum, o *newsfeeds (5)* página do manual irá explicar o uso do `param` campo em alguns detalhes.

Há um nome do site especial que deve ser codificado como `ME` e deve ser a primeira entrada no arquivo. Esta entrada é usada para controlar as configurações padrão para seus feeds. Se o `ME` entrada tem uma lista de distribuição associadas a ele, esta lista será anteposto a cada uma das entradas outro site antes de serem enviados. Isto permite-lhe, por exemplo, declare alguns grupos de notícias para serem alimentados automaticamente, ou automaticamente impedido de alimentação, sem ter de repetir
o padrão em cada entrada do site.

Mencionamos anteriormente que era possível utilizar alguns alimentos especiais para gerar dados de segmento que faz a notícia-Emprego leitor mais fácil. Faremos isso através da exploração do `overchan` comando que é parte da distribuição do DCI. Para fazer isso, criamos um feed local especial chamado `Resumo` que vai passar as notícias para o `overchan`
comando para processamento de dados em síntese.

Nosso servidor de notícias irá fornecer apenas um feed de notícias externas, que vai para a Universidade de Groucho Marx, e

eles
receber artigos para todos os grupos de notícias, exceto o *controle* e *lixo* newsgroups, o *rec.crafts.brewing.private* notícias grupo, que serão mantidos no local, e os *rec.crafts.brewing.poison* newsgroup, que nós não queremos que as pessoas de nossa cervejaria visita postando.

Usaremos o `nntpsend` comando para o transporte de notícias via NNTP para o *news.groucho.edu* servidor.
`nntpsend` nos obriga a usar o "arquivo" método de entrega e escrever caminho do texto e identificação do artigo. Nota que nós definir o *param* campo para o nome do arquivo de saída. Vamos falar um pouco mais sobre o `nntpsend` commando em um momento. Nosso newsfeed configuração resultante é:

```
# / News / etc / newsfeeds arquivo para a Cervejaria Virtual
#
# Envia todos os grupos de notícias, exceto os de controle e lixo por defeito
ME:! Controle, junk::
#
# Resumo Gerar dados para qualquer locutores de usar.
Resumo: Tc, WO: / usr / lib / news / bin / overchan
#
# Alimente o Groucho Marx tudo, exceto nosso newsgroup Universidade privada
# E todos os artigos postados no newsgroup rec.crafts.brewing.poison.
gmarxu! rec.crafts.brewing.poison, @ rec.crafts.brewing.private: \
        Tf, WNM: news.groucho.edu
#
```

O arquivo nntpsend.ctl

A `nntpsend` programa controla a transmissão de notícias usando o protocolo NNTP, chamando o
`innxmit` comando. Vimos um uso simples da `nntpsend` comando anterior, mas ele também tem uma configuração arquivo que nos proporciona uma certa flexibilidade na forma como configurar o nosso feeds de notícias.

A `nntpsend` comando espera encontrar arquivos em lotes para os locais que irão alimentar. Ele espera que esses arquivos em

lote a ser
nomeado */ Var / spool / news / sitename / out.going*.`innd` cria esses arquivos em lote, quando agindo em uma entrada no *notícias feeds*, O que vimos nas seções anteriores. Nós especificamos o nome do site como o nome do arquivo no *param* campo, e que satisfaz a `nntpsend` requisitos de comando de entrada.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A `nntpsend` comando tem um arquivo de configuração chamado *nntpsend.ctl* que normalmente é armazenado no */ Notícias / etc /* diretório.

A *nntpsend.ctl* arquivo nos permite associar um nome de domínio totalmente qualificado, algumas notícias restrições de tamanho de ração, e uma
número de parâmetros de transmissão com um nome de site de notícias feed. O nome do site é um meio de identificar unicamente
uma alimentação lógica de artigos. O formato geral do arquivo é:

```
sitename: fqdn: [args]: max_size
```

A lista a seguir descreve os elementos desse formato:

sitename

O nome do site como fornecido no *newsfeeds* arquivo

fqdn

O nome de domínio totalmente qualificado do servidor de notícias em que vamos estar a alimentar as notícias

max_size

O volume máximo de notícia para se alimentar de qualquer transferência única

args

Os argumentos adicionais para passar para o `innxmit` comando

Nosso exemplo de configuração requer um muito simples *nntpsend.ctl* arquivo. Temos apenas um feed de notícias. Nós vamos

limitar a
ração a um máximo de 2 MB de tráfego e vamos passar um argumento para a `innxmit` que define a 3 minutos (180 segundo) tempo limite. Se fôssemos um site maior e tinha muitos novos feeds, nós simplesmente criar novas entradas para cada novo
site de alimentação que parecia muito a mesma que esta:

```
# / News / etc / nntpsend.ctl
#
gmarxu: news.groucho.edu: 2m: t-180
#
```

Controlando o acesso Newsreader

Não muitos anos atrás, era comum que as organizações forneçam acesso do público aos seus servidores de notícias. Hoje é difícil de localizar servidores de notícias públicos, a maioria das organizações cuidadosamente controlar quem tem acesso aos seus servidores,
geralmente restringem o acesso aos usuários suportados na sua rede. DCI fornece arquivos de configuração para o controle dessa acesso.

O arquivo incoming.conf

Nós mencionamos em nossa introdução ao DCI que atinge cerca de sua eficiência e tamanho, separando as notícias mecanismo de alimentação do mecanismo de newsreading. A */ Notícias / etc / incoming.conf* arquivo é onde você especifica qual Exércitos estará alimentando-lhe a notícia usando o protocolo NNTP, bem como onde você define alguns parâmetros que controlar a forma como os artigos são alimentados a partir de você nestes hospedeiros. Qualquer host não mencionados neste arquivo que se conecta à notícia
tomada não será tratado pelo `innd` daemon, em vez disso, ele será tratado pelo `nnrpd` daemon.

A */ Notícias / etc / incoming.conf* sintaxe do arquivo é muito simples, mas leva um tempo para vir aos termos com. Três tipos de entradas válidas são permitidos: pares chave / valor, que são como você especificar atributos e seus valores, seus pares, que É assim que você especifique o nome de um host permitido enviar artigos para nós usando NNTP e grupos, um meio de aplicar-ing chave / valor pares para grupos de pares. Pares chave / valor pode ter três diferentes tipos de escopo. pares Global ap-dobra a cada ponto definido no arquivo. pares Grupo aplica a todos os pares definidos dentro desse grupo. pares Peer aplicar apenas a esse ponto um. definições específicas substituir os menos específicos: por isso, substituir as definições do grupo de pares
definições, que por sua vez, sobrepor os pares globais.

Chaveta de caracteres (`{}`) São usados para delimitar o início eo fim do `grupo` e `pares` especificações. O #
personagem marca o resto da linha que aparece como um comentário. Pares chave / valor são separados por dois pontos caracc-cional e aparecem uma a uma linha.

Um certo número de chaves diferentes pode ser especificado. Os mais comuns e úteis são:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

hostname

Essa chave especifica uma lista separada por vírgulas de nomes totalmente qualificados ou endereços IP dos pares que nós vamos
permitem enviar-nos artigos. Se essa chave não é fornecida, os padrões hostname para o rótulo do par.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

streaming

Essa chave determina se os comandos de streaming são permitidas a partir deste host. É um valor booleano que padrões para `verdade`.

max-conexões

Essa chave especifica o número máximo de conexões permitidas a partir deste grupo ou de pares. Um valor de zero significa ilimitado (que também pode ser especificado usando `none`).

senha

Essa chave permite que você especifique a senha que deve ser utilizado por um colega se for para ser autorizado a transferir notícias. O padrão é não exigir uma senha.

padrões

Essa chave especifica o newsgroups que aceitamos a partir de pares associados. Este campo é codificado de acordo precisamente as mesmas regras que usamos em nossas *newsfeeds* arquivo.

Em nosso exemplo, temos apenas uma máquina que estamos esperando para nos alimentar de notícias: o nosso fornecedor de notícias para montante
Groucho Marx Universidade. Nós vamos ter nenhuma senha, mas vamos garantir que nós não aceitamos nenhum artigo para a nossa
privado de notícias do exterior. Nossa *hosts.nntp* olha como:

```
# Virtual arquivo incoming.conf Brewery.

# As configurações globais
streaming:       verdade
max-conexões: 5

# Permitir NNTP postagem do nosso host local.
pares {ME
    hostname: "localhost, 127.0.0.1"
}

# Permitir groucho para nos enviar todos os grupos de notícias, exceto os nossos entes
locais.
peer groucho {
    hostname: news.groucho.edu
    padrões! rec.crafts.brewing.private
}
```

O arquivo nnrp.access

Mencionamos anteriormente que os locutores, e na verdade não qualquer host listado na *hosts.nntp*, Que se conectam ao DCI servidor de notícias são tratadas pelo `nnrpd` programa. `nnrpd` usa o */ Notícias / etc / nnrp.access* arquivo para determinar quem é permissão para fazer uso do servidor de notícias, e as permissões que eles devem ter.

A *nnrp.access* arquivo tem uma estrutura semelhante a outros arquivos de configuração que temos olhado. É composto por um conjunto de padrões utilizados para o jogo contra o nome do host de conexão de domínio ou endereço IP, e os campos que determinam o que acesso e permissão deve ser dada. Cada entrada deve aparecer em uma linha por si só, e os campos são separados por dois pontos. A última entrada neste arquivo que corresponde ao host de conexão será o utilizado, então, novamente, você deve colocar padrões gerais em primeiro lugar e segui-los com outros mais específicos no final do arquivo. Os cinco campos de cada entrada na ordem que deve aparecer são:

Hostname ou endereço IP

Este campo está de acordo com *wildmat (3)* regras de correspondência de padrão. É um padrão que descreve a conexão nome do host ou o endereço IP.

Permissões

Este campo determina quais permissões o host correspondente deve ser concedida. Há dois permissons você pode configurar: `R` dá permissões de leitura e `P` dá permissões de postagem.

Nome de Usuário

Este campo é opcional e permite que você especifique um nome de usuário que um cliente NNTP deve fazer logon no

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

servidor
antes de serem autorizados a postar notícias. Esse campo pode ser deixado em branco. Nenhuma autenticação de usuário é re-
cessária para ler artigos.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Senha

Este campo é opcional e é a senha que acompanha o *username* de campo. Deixando este campo em branco significa que a senha não é necessária para postar artigos.

Grupos de notícias

Este campo é um padrão que especifica quais newsgroups o cliente tem permissão para acessar. O padrão segue as mesmas regras que as utilizadas no *newsfeeds* arquivo. O padrão para este campo não é newsgroups, para que normalmente têm um padrão configurado aqui.

No exemplo a fábrica de cerveja virtual, que permitirá que qualquer cliente NNTP no domínio Cervejaria Virtual para ler e pós a todos os newsgroups. Vamos permitir que qualquer cliente NNTP acesso somente leitura a todos os newsgroups, exceto nosso privada
notícias internas. Nossa *nnrp.access* arquivo será parecido com este:

```
# Virtual Cervejaria - nnrp.access
# Vamos permitir a leitura pública de todas as notícias, exceto nosso privada.
*: R :::*,! rec.crafts.brewing.private

# Qualquer máquina com o domínio Cervejaria Virtual pode ler e enviar a todos os
newsgroups #
*. Vbrew.com: RP:: *
```

Vencer Notícias

Quando os artigos de notícias são recebidas por um servidor de notícias, elas são armazenadas no disco. Artigos de notícias

precisam estar disponíveis para
usuários de um determinado período de tempo para ser útil, assim que um servidor de notícias grande operação pode consumir muito espaço em disco. Para
garantir que o espaço em disco é utilizado de forma eficaz, você pode optar por apagar artigos de notícia automaticamente após um período de
tempo. Isso é chamado `vencimento artigo`. Naturalmente, a pousada proporciona um meio de notícias que termina automaticamente
artigos.

O arquivo expire.ctl

O servidor DCI usa um programa chamado `expirar` para excluir expirou notícias. A `expirar` programa, por sua vez usa um arquivo chamado */ Notícias / etc / expire.ctl* para configurar as regras que governam a expiração artigo.

A sintaxe da */ Notícias / etc / expire.ctl* é bastante simples. Tal como acontece com a maioria dos arquivos de configuração, as

linhas em branco ou linhas de começar-
ning com o caractere # são ignorados. A idéia geral é que você especificar uma regra por linha. Cada regra define como vencimento artigo será realizada em grupos de correspondência de um padrão fornecido. A sintaxe da regra parece isso:

padrão : *modflag* : *manter* : *padrão* : *purga*

A lista a seguir descreve os campos:

padrão

Este campo é uma lista delimitada por vírgula dos padrões de correspondência entre os nomes de grupos de notícias. A *wildmat*(3) de rotina
é usado para corresponder a esses padrões. A regra anterior um nome de newsgroup é aquele que é aplicado, por isso, se pretende especificar curinga (*) regras, devem ser listadas primeiro neste arquivo.

modflag

Esta bandeira descreve como esta regra se aplica a grupos de notícias moderado. Ele pode ser codificado com um `M` a média
que esta regra só se aplica a grupos de notícias moderado, uma `U` para dizer que esta regra só se aplica aos unmoder-newsgroups operado, ou de um `A` para dizer que esta regra ignora o estado moderado e se aplica a todos os grupos.

manter

Este campo permite que você especifique o tempo mínimo de um artigo com um "Expira" cabeçalho será mantido se-
ja quanto é expirado. As unidades são dias, e são um ponto flutuante, assim você pode especificar valores como `7.5`

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

para
sete dias e meio. Você também pode especificar `nunca` Se você deseja artigos para ficar em um newsgroup para sempre.

padrão

Este campo é o mais importante. Este campo permite que você especifique o tempo de um artigo sem `Ex-Pires` cabeçalho será mantido. A maioria dos artigos não terá um `Expira` cabeçalho. Este campo é codificado na mesma forma que o *manter* campo, com `nunca` o que significa que os artigos sem `Expira` cabeçalhos nunca será expirado.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

purga

Este campo permite que você especifique o tempo máximo de um artigo com uma `Expira` cabeçalho será mantido se- portanto é expirado. A codificação deste campo é a mesma para o `manter` de campo.

Nossas exigências são simples. Vamos manter todos os artigos em todos os newsgroups para 14 dias por padrão, e entre 7 e 21 dias para os artigos que têm uma `Expira` cabeçalho. A *rec.crafts.brewing.private* newsgroup é o nosso interno newsgroup, por isso vamos ter certeza de que não expiram todos os artigos dele:

```
# Arquivo expire.ctl para a Cervejaria Virtual

# Vence todos os artigos em 14 dias, por padrão, 7-21 dias para aqueles com
# Expira: cabeçalhos
*: A: 07:14:21

# Este é um grupo de discussão interna especial, que nunca irá expirar.
rec.crafts.brewing.private: A: nunca: nunca: nunca
```

Vamos mencionar um tipo especial de entrada que você pode ter em sua */ Notícias / etc / expires.ctl* arquivo. Você pode ter exatamente
uma linha parecida com esta:

`/ Lembre /:`*dia*

Esta entrada permite que você especifique o número mínimo de dias que um artigo será lembrado na história arquivo, independentemente de o próprio artigo tem sido expirado ou não. Isso pode ser útil se um dos sites que está se alimentando artigos é infreqüente e tem o hábito de enviar artigos antigos e agora cada vez. Definir o */ Lembre /* campo ajuda a evitar que o servidor upstream de lhe enviar o artigo novamente, mesmo se já tiver sido expirado a partir do seu servidor. Se o servidor se lembra que já recebeu o artigo, ele irá rejeitar as tentativas reenviá-la. É importante lembrar que essa configuração não tem efeito algum sobre a validade do artigo, que afeta apenas o tempo que os detalhes de um artigo são mantidos no banco de dados da história.

Manipulação de mensagens de controle

Assim como com o C News, DCI pode processar automaticamente mensagens de controle. INN oferece uma configuração poderosa
mecanismo para controlar a ação ocorrerá para cada um de uma variedade de mensagens de controle, e um controle de acesso mecanismo para controlar quem pode iniciar ações contra as quais newsgroups.

O arquivo control.ctl

A *control.ctl* arquivo é bastante simples na sua estrutura. As regras de sintaxe para esse arquivo são os mesmos que para os restantes
arquivos de configuração do DCI. Linhas que começam com # são ignorados, as linhas podem ser mantidas com `/`, E os campos são de-
limitado pela `:`.

Quando uma mensagem de controle é recebida, ela é testada contra cada regra de cada vez. A última regra no arquivo que corresponda ao
mensagem é a regra que será usado, então você deve colocar regras genéricas no início do arquivo e mais específica regras no final do arquivo. A sintaxe geral do arquivo é:

Mensagem`:`*a partir de*`:`*newsgroups*`:`*ação*

Os significados de cada um dos campos são:

Mensagem

Este é o nome da mensagem de controle. mensagens de controle típicos são descritos mais adiante.

a partir de

Este é um padrão shell-estilo que combine com o endereço de e-mail da pessoa que envia a mensagem. O e-mail endereço é convertido para minúsculas antes de comparação.

newsgroups

Se a mensagem de controle é `newgroup` ou `rmgroup`, Este campo é um padrão shell-estilo que combine com a notícia-

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Grupo criado ou removido.

ação

Este campo especifica qual ação a ser tomada por qualquer mensagem correspondente à regra. Há um bom número de ações que podemos tomar, são descritas na lista ao lado.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

A *Mensagem* campo de cada linha pode ter um dos seguintes valores:

checkgroups

Esta mensagem solicita que os administradores do seu banco de dados de notícias resynchonrize newsgroups ativa contra
a lista de grupos fornecido na mensagem de controle.

newgroup

Esta mensagem solicita que a criação de um novo grupo. O corpo da mensagem de controle deve conmanter uma breve descrição do propósito do grupo de notícias a ser criado.

rmgroup

solicita que um grupo de discussão ser removido.

sendsys

Esta mensagem solicita que o *sys* arquivo deste servidor notícia ser transmitida por e-mail para o autor da controle da mensagem. RFC-1036 afirma que é uma exigência da adesão da Usenet que esta informação estar disponíveis ao público, pois é usado para manter o mapa da Usenet até à data.

versão

Esta mensagem solicita que o nome da máquina ea versão do software servidor de notícias ser devolvido ao originator da mensagem de controle.

todos

Esta é uma codificação especial que irá corresponder a qualquer mensagem de controle.

A *Mensagem* domínio pode incluir as seguintes ações:

bagatela

O comando solicitado é executado. Em muitos casos, uma mensagem de e-mail será enviado para o administrador aconselhá-los de que a ação ocorreu.

func =*arquivo*

Este é o mesmo que o `bagatela` ação, exceto que uma mensagem de log será gravada no *arquivo* arquivo de log. Se o arquivo especificado está *e-mail*, A entrada de log é enviado por e-mail. Se o arquivo especificado é a cadeia nula, o show-log
Sábio é gravado */ Dev / null* e é equivalente a usar a incondicional `bagatela` acção. Se o *arquivo* nome sergins com um caractere /, o nome é considerado um nome de arquivo absoluto para o arquivo de log, caso contrário, especi-
cados nome é traduzido para o */ Var / log / news / file.log*.

doifarg

O comando solicitado é executado se o comando tem um argumento. Se o comando não tem argumento, a mensagem de controle é ignorada.

queda

O comando solicitado é ignorado.

log

Uma mensagem de log é enviada para o `stderr` saída do `innd` processo. Isso normalmente é direcionado para fora do
/ Var / log / news / errlog arquivo.

= log*arquivo*

Este é o mesmo que um `log` ação, exceto o arquivo de log é especificado de acordo com as normas estabelecidas para o `bagatela`=*arquivo*
acção.

e-mail

Uma mensagem de e-mail é enviado para o administrador da notícia que contém os detalhes comando solicitado. Nenhum outro ação acontece.

verificar-*

Se uma ação começa com a string "`verificar-`", Então a mensagem de controle é autenticado usando PGP (ou GPG).[139]

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

139 PGP e GPG são ferramentas projetadas para autenticar ou criptografar mensagens usando técnicas de chave pública. BPM é a versão do GNU livre do PGP. GPG pode ser encontrado em http://www.gnupg.org/E PGP podem ser encontradas em http://www.pgp.com/.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Para que você possa ver o que um *control.ctl* arquivo ficaria assim, na prática, aqui está uma amostra muito pequena ilustrativo:

```
# # Exemplo / noticias / etc / control.ctl
# #
# # Atenção: Você não deve usar esse arquivo, ele é somente ilustrativo.

# #     Controle de manipulação de mensagens
todos os emails :*:*:
checkgroups :*:*: mail
queda :*:*: ihave
queda :*:*: sendme
sendsys log :*:*: = sendsys
log :*:*: senduuname = senduuname
log versão :*:*: = versão
newgroup mail :*:*:
rmgroup mail :*:*:

# # mensagens de controle do punho para as oito heirarchies notícia mais importante
# # COMP, humanidades, MISC, NEWS REC, SIC, Talk, SOC
check-
grupos: *: soltar: comp .* | Discussão humanas .* .* | misc .* | notícias .* | rec .*
| sci .* | | soc .*
newgroup *: comp .* | humanidades .* | misc .* | notícias .* | rec .* | sci .* |
Discussão .* | soc .*: queda
rmgroup: *: comp .* | humanidades .* | misc .* | notícias .* | rec .* | sci .* |
Discussão .* | soc .*: queda
checkgroups: group-admin@isc.org: *: verificar-news.announce.newgroups
newgroup: comp .* | misc .* | notícias .*:: group-admin@isc.org verificar-
news.announce.newgroups
newgroup: group-admin@isc.org: rec .* | sci .* | soc .*: verificar-
news.announce.newgroups
newgroup: group-admin@isc.org: Discussão .* | humanidades .*: verificar-
news.announce.newgroups
rmgroup: comp .* | misc .* | notícias .*:: group-admin@isc.org verificar-
news.announce.newgroups
rmgroup: group-admin@isc.org: rec .* | sci .* | soc .*: verificar-
news.announce.newgroups
rmgroup: group-admin@isc.org: Discussão .* | humanidades .*: verificar-
news.announce.newgroups

# # GNU (Free Software Foundation)
newgroup: gnu .*:: gnu@prep.ai.mit.edu doit
newgroup: noticias ai.mit.edu * @ gnu .*: doit
rmgroup: gnu .*:: gnu@prep.ai.mit.edu doit
rmgroup: noticias ai.mit.edu * @ gnu .*: doit

# # Linux (Newsfeed de news.lameter.com)
checkgroups: christoph@lameter.com: linux .*: doit
newgroup: linux .*:: christoph@lameter.com doit
rmgroup: linux .*:: christoph@lameter.com doit
```

Correndo DCI

A `estalagem` pacote fonte fornece um script adequado para o início `estalagem` em tempo de boot. O roteiro é normalmente

chamado
/ Usr / lib / news / bin / rc.news. O script lê os argumentos de um outro script, normalmente chamado
/ Usr / news / lib / innshellvars, Que contém as definições dos nomes e caminhos de arquivos que `estalagem` será usado para localizar
componentes necessários. É geralmente considerada uma boa idéia para executar `estalagem` com as permissões de um não-raiz
usuário, como `notícias`.

Para garantir que `estalagem` é iniciado no tempo de boot, você deve verificar se */ Usr / news / lib / innshellvars* é cor-
configurado

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

corretamente e, em seguida, chamar o */ Usr / lib / news / bin / rc.news* script de um script executado durante a inicialização.

Além disso, existem tarefas administrativas que devem ser realizados periodicamente. Estas tarefas são normalmente config-
tem de ser configurada para ser executada pelo `cron` comando. A melhor maneira de fazer isso é adicionar os comandos
apropriados para o seu

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

/ Etc / crontab arquivo, ou melhor ainda, criar um arquivo adequado para o */ Etc / cron.d* diretório, se a sua distribuição fornece um. Um exemplo de tal arquivo pode parecer:

```
# Exemplo de arquivo / etc / cron.d pousada, como usado na distribuição Debian.
#
SHELL = / bin / sh
PATH = / usr / lib / news / bin: / sbin: / bin: / usr / sbin: / usr / bin

# Vence notícia velha e entradas de visão noturna, gerar relatórios.

15 * * 0 *      notícia news.daily expireover lowmark delayrm
                s

# A cada hora, executar uma rnews-U. Este não é apenas para sites UUCP, mas
# Também a processo na fila artigos colocados lá por in.nnrpd no caso
# Innd não estava aceitando todos os artigos.

10 * * * *      notícia rnews-U
                s
```

Esses comandos irão assegurar que as notícias de idade é automaticamente terminado a cada dia, e que todos os artigos estão na fila
processados a cada hora. Note também que eles são executados com as permissões do `notícias` usuário.

Gerenciando DCI: O comando ctlinnd

O servidor de notícias INN vem com um comando para gerenciar suas operações do dia-a-dia. A `ctlinnd` comando pode ser usada para manipular grupos de notícias e feeds de notícias, para obter o status, do servidor, e para recarregar, parada, e iniciar o servidor.

Você costuma receber um resumo das `ctlinnd` sintaxe de comando usando:

Ctlinnd-h

Nós vamos cobrir alguns dos usos mais importantes do `ctlinnd` aqui, por favor consulte o `ctlinnd` página do manual para detalhes.

Adicionar um novo grupo

Use a seguinte sintaxe para adicionar um novo grupo:

`ctlinnd newgroup` *criador do resto do grupo*

Os argumentos são definidos como segue:

grupo

O nome do grupo para criar.

descanso

Este argumento deve ser codificada da mesma forma como o *bandeiras* domínio da *ativos* arquivo. O padrão é `y` se não fornecido.

criador

O nome da pessoa que cria o grupo. Coloque-a entre aspas se houver espaços no nome.

Alterar um Grupo

Use a seguinte sintaxe para alterar um grupo:

`ctlinnd changegroup` *resto do grupo*

Os argumentos são definidos como segue:

grupo

O nome do grupo para a mudança.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

descans

o Este argumento deve ser codificada da mesma forma como o *bandeiras* domínio da *ativos* arquivo.

Esse comando é útil para mudar o status de moderação de um grupo.

Remover um grupo

Use a seguinte sintaxe para remover um grupo:

`ctlinnd rmgroup` *grupo*

O argumento é definido como segue:

grupo

O nome do grupo a ser removido.

Este comando remove o newsgroup especificado a partir de *ativos* arquivo. Não tem nenhum efeito sobre o spool de notícias.

Todos os artigos do carretel para o grupo especificado será expirado na forma usual, mas sem novos artigos serão aceitas.

Renumerar um Grupo

Use a seguinte sintaxe para numerar um grupo:

`renumerar ctlinnd` *grupo*

O argumento é definido como segue:

grupo

O nome do grupo para numerar. Se um `grupo` é uma seqüência vazia, todos os grupos são numeradas.

Este comando atualiza a marca d'água baixa para o grupo especificado.

Permitir / Bloquear Newsreaders

Use a seguinte sintaxe para permitir ou não locutores:

`leitores ctlinnd` *Texto da bandeira*

Os argumentos são definidos como segue:

pavilhão

Especificando `n` faz com que todas as conexões de newsgroups para ser proibido. Especificando `y` permite con-leitor conexões.

texto

O texto fornecido será dada aos leitores de notícias que tentam se conectar, e geralmente descreve o motivo para desabilitar o acesso newsreader. Ao reativar o acesso leitor, este campo deve ser um vazio seqüência ou uma cópia do texto fornecido quando o leitor foi desativada.

Este comando não afeta newsfeeds entrada. Ele só controla as conexões de locutores.

Rejeitar Newsfeed Conexões

Use a seguinte sintaxe para rejeitar conexões newsfeed:

`ctlinnd rejeitar` *razão*

O argumento é definido como segue:

razão

O texto fornecido deve explicar por que as ligações recebidas para `innd` são rejeitadas.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Este comando não afeta as conexões que são entregues à `nnrpd` (Ou seja, leitores de notícias), que só affects conexões que seria tratado pelo `innd` diretamente, como newsfeeds remoto.

Permitir conexões Newsfeed

Use a seguinte sintaxe para permitir conexões newsfeed:

`ctlinnd permitir` *razão*

O argumento é definido como segue:

razão

O texto fornecido deve ser o mesmo que o fornecido ao anterior `rejeitar` comando ou um vazio string.

Este comando reverte o efeito de uma `rejeitar` comando.

Desative o servidor Notícias

Use a seguinte sintaxe para desativar o servidor de notícias:

`acelerador ctlinnd` *razão*

O argumento é definido como segue:

razão

A razão para a otimização do servidor.

Este comando é, simultaneamente, equivalente a um `locutores não` e um `rejeitar`, E é útil quando o trabalho de emergência é realizado no banco de dados de notícias. Ele garante que as tentativas nada para atualizá-lo
enquanto você está trabalhando nisso.

Reinicie o servidor de notícias

Use a seguinte sintaxe para reiniciar o servidor de notícias:

`ctlinnd ir` *razão*

O argumento é definido como segue:

razão

A razão dada quando parar o servidor. Se este campo é uma seqüência vazia, o servidor será reativado incondicionalmente. Se uma razão é dada, apenas aquelas funções com deficiência com uma razão correspondente ao fornecido
texto será reiniciado.

Este comando é usado para reiniciar um servidor de função após uma `regulador de pressão`,`pausa`Ou

`rejeitar` comando.

Tela de status de um Newsfeed

Use a seguinte sintaxe para exibir o status de um newsfeed:

`feedinfo ctlinnd` *site*

O argumento é definido como segue:

site

O nome do site (retirado da *newsfeeds* arquivo) para o qual você deseja exibir o status de newsfeed.

Largar um Newsfeed

Use a seguinte sintaxe para soltar um newsfeed:

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

`queda ctlinnd` *site*

O argumento é definido como segue:

site

O nome do site (retirado da *newsfeeds* arquivo) para que se alimenta são descartados. Se este campo estiver vazio seqüência, todos os feeds activos serão descartados.

Soltando um newsfeed a um pára qualquer site feeds activos para o site. Não é uma mudança permanente. Essa comando seria útil se você tiver modificado os detalhes feed de um site e um feed para o site está ativo.

Comece um Newsfeed

Use a seguinte sintaxe para iniciar um newsfeed:

`ctlinnd começar` *site*

O argumento é definido como segue:

site

O nome do site a partir do *newsfeeds* arquivo para que se alimenta são iniciados. Se um avanço para o site já está activa, uma `queda` comando é feito primeiro automaticamente.

Este comando faz com que o servidor para reler o *newsfeeds* arquivo, localize a entrada de correspondência, e iniciar as um newsfeed para o site chamado utilizando os dados encontrados. Você pode usar este comando para testar um novo feed de notícias
a um site depois que você adicionou ou alterou a sua entrada no *newsfeeds* arquivo.

Cancelar um artigo

Use a seguinte sintaxe para cancelar um artigo:

`ctlinnd cancelar` *Message-Id*

O argumento é definido como segue:

Message-ID

A identificação do artigo a ser cancelado.

Este comando faz com que o artigo específico a ser excluído do servidor. Não gera um cancelamento mensagem.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Capítulo 24 - Configuração Newsreader

A `newsreader` é um programa que os usuários invocar para visualizar, armazenar e criar artigos. Vários locutores foram portados para o Linux. Vamos descrever a configuração básica para os três locutores mais populares: `estanho`,`trn`, e `nn`.

Um dos locutores mais eficaz é:

```
$ find / var / spool / news-name '[0-9] * "-exec cat {} \; | mais
```

Este é o caminho Unix die-hards ler suas notícias.

A maioria dos leitores de notícias, no entanto, são muito mais sofisticados. Eles normalmente oferecem uma interface de tela cheia com sepa- níveis de taxa para a exibição de todos os grupos que o usuário tenha subscrito, uma visão geral de todos os artigos em cada grupo, e artigos individuais. Muitos navegadores da Web dupla como locutores, mas se você quiser usar um leitor autônomo, Este capítulo explica como configurar os dois clássicos: `trn` e `nn`.

Ao nível de notícias, a maioria dos locutores exibir uma lista de artigos, mostrando suas linhas de assunto e autores. Em grandes grupos, é difícil para o usuário acompanhar artigos relacionados uns aos outros, embora seja possível identificar respostas aos artigos anteriores.

A resposta geralmente repete o assunto do artigo original, precedendo-a com `Re:`. Além disso, o `Consulte-diferenças:` linha do cabeçalho deve incluir a identificação da mensagem do artigo em que a resposta está diretamente seguimento.
Classificando artigos escritos por estes dois critérios gera pequenos aglomerados (na verdade, árvores) de artigos, que são chamados *tópicos*.
Uma das funções da escrita é um leitor de notícias elaboração de um sistema eficiente de segmentação, pois o tempo necessário para isso é proporcional ao quadrado do número de artigos.

Não vou entrar em como as interfaces de usuário são construídas aqui. Todos os leitores de notícias disponíveis atualmente para o Linux tem um função de uma boa ajuda, por favor consultá-lo para obter mais detalhes.

Nas seções seguintes, vamos lidar somente com tarefas administrativas. A maioria destes referem-se a criação de tópicos bases de dados e contabilidade.

Configuração de estanho

O leitor mais versátil no que diz respeito a segmentação é `estanho`. Foi escrita por Iain Lea e é vagamente mod- ram com um velho chamado newsreader `tass` (Escrito por Rich Skrenta). Ele faz a sua segmentação quando o usuário entra o grupo de notícias, e é muito rápido, a menos que você está recebendo mensagens via NNTP.

Em uma configuração: 486DX50, que leva aproximadamente 30 segundos para discussão 1.000 artigos ao ler diretamente do disco. Seria demorar mais de 5 minutos sobre NNTP para chegar a um servidor de notícias carregadas.[140] Você pode melhorar este tempo regularmente atualizar o arquivo de índice, invocando `estanho` com o *-U* opção, para que quando você começar a próxima `estanho` para ler a notícia tópicos já existentes. Alternativamente, você pode invocar `estanho` com o *-U* opção para ler notícias. Quando invocado este forma, `estanho` garfos de um processo de fundo para criar o índice arquivos enquanto você estiver lendo notícias.

Normalmente, `estanho` descarrega seus bancos de dados de segmentação no diretório home do usuário abaixo *.tin / index*. Isso pode ser dispendiosa em termos de recursos, entretanto, assim que você deve manter uma única cópia deles em um local central. Isso pode ser obtém-se fazendo `estanho` setuid para *notícias*, Por exemplo. `estanho` então vai manter todos os bancos de discussão abaixo */ Var / spool / news / .index*. Para qualquer fuga de acesso a arquivos ou shell, que vai redefinir o seu uid efetivo para o UID real do usuário

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

que o invocou.[141]

A versão do `estanho` incluído em algumas distribuições Linux é compilado sem suporte NNTP, mas a maioria tem isso agora. Quando invocado como `rtin` ou com o *-R* opção, `estanho` tenta se conectar ao servidor NNTP especificado no arquivo */ NNTPSERVER / etc* ou no *NNTPSERVER* variável de ambiente. A *NNTPSERVER* arquivo simplesmente contém o servidor nome em uma única linha.

140 As coisas melhoram drasticamente se o servidor NNTP que a segmentação em si e permite ao cliente recuperar as linhas bases de dados; DCI faz isso, por exemplo.

141 Esta é a razão pela qual você vai receber mensagens de erro feio quando invocando `estanho` como superusuário. Mas você não deve fazer o trabalho de rotina como *root*, de qualquer maneira.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Configuração trn

`trn` É também o sucessor de um antigo leitor, ou seja, `rn` (O que significa *ler notícias*). O "t" no nome significa "rosca". Foi escrito por Wayne Davidson.

Diferentemente `estanho`,`trn` não tem nenhuma disposição para gerar seu banco de dados de segmentação em tempo de execução. Em vez disso, ele usa os pré-comparada por um programa chamado `mthreads` que tem de ser invocado regularmente a partir de `cron` para atualizar os arquivos de índice.

Você ainda pode acessar os novos artigos, se você não estiver executando `mthreads`, Mas você vai ter todas essas "A VERDADEIRA OPORTUNIDADE DE INVESTIMENTO "artigos espalhados por todo o seu menu de selecção do artigo, em vez de um único segmento você pode facilmente pular.

Para ativar threading para newsgroups especial, invocar `mthreads` com a lista de grupos no comando linha. O formato da lista é a mesma que a do C News *sys* arquivo:

```
$ 'Comp, rec,! Rec.games.go' mthreads
```

Este comando permite segmentação para todos os comp e rec, exceto para rec.games.go (pessoas que jogam Go não necessidade tópicos fantasia). Depois disso, basta invocar `mthreads` sem opções em tudo para fazer qualquer nova discussão chegou artigos. Segmentação de todos os grupos encontrados em seu *ativos* arquivo pode ser ativada por chamar `mthreads` com uma lista de grupo de todos.

Se você está recebendo a notícia durante a noite, você costuma executar `mthreads` uma vez de manhã, mas você pode também a fazê-lo com mais freqüência, se necessário. Sites que tem um tráfego muito pesado pode querer correr `mthreads` em daemon modo. Quando ele é iniciado no tempo inicializar usando o *-D* opção, ele se coloca em segundo plano, acorda a cada dez minutos para verificar se existem artigos recém-chegados, e os tópicos. Para executar `mthreads` no DAE-Modo de seg, coloque a seguinte linha no seu *rc.news* script:

```
/ Usr / local / bin / RN / mthreads deav-
```

A *-Um* opção faz com que `mthreads` ligar automaticamente segmentação para novos grupos, elas são criadas; *-V* permite verbose mensagens de log para o `mthreads` arquivo de log *mt.log* no diretório onde você tem `trn` instalado.

artigos antigos que não estão mais disponíveis deve ser removido do índice de arquivos regularmente. Por padrão, apenas os artigos com um número abaixo da marca de água de baixa será removida.[142] Artigos acima deste número que tem sido expirado (Porque o artigo mais antigo foi atribuída uma data de expiração de comprimento por um *Expira em:* campo de cabeçalho), podem ser removidos, dando- `mthreads` o *-E* opção para forçar uma execução do termo "reforço". Quando `mthreads` está executando em modo daemon, o *-E* opção faz com que `mthreads` posto em tal termo um reforço executado uma vez por dia, pouco depois meia-noite.

Configuração nn

`nn`, Escrito por Kim Storm F., diz ser um leitor de notícias cujo objetivo final não é para ler notícias. Seu nome significa para "No News", e seu lema é "Nenhuma notícia é boa notícia. `nn` é melhor. "

Para alcançar este objectivo ambicioso, `nn` vem com uma grande variedade de ferramentas de manutenção que não só permitem segmento de geração, mas também verificações de consistência extenso banco de dados, contabilidade, recolha de estatísticas de uso e ~~restrições de acesso. Existe também~~ um programa de administração chamado `nnadmin`, Que permite que você execute essas tarefas de forma interativa. É muito intuitivo, por isso não vamos insistir sobre estes aspectos, mas apenas lidar com a geração de os arquivos de índice.

A `nn` tópicos gerente de banco de dados é chamado `nnmaster`. Ele geralmente é executado como um daemon, iniciado a partir

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

de uma *rc* arquivo em
tempo de inicialização. É invocado como:

```
/ Usr / local / nn / lib / nnmaster-l-r-C
```

Isso permite segmentação para todos os newsgroups presentes no seu *ativos* arquivo.

Equivalentemente, pode invocar `nnmaster` periodicamente a partir `cron`, Dando-lhe uma lista de grupos para agir. Este lista é muito semelhante à lista de subscrição no *sys* arquivo, exceto que ele usa espaços em branco em vez de vírgulas. Em vez de

142 Note-se que C News (descrito no Capítulo 21, *C News*) Não atualização desta marca de água de baixa automaticamente, você tem que executar `updatemin` fazê-lo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

o nome do grupo falso todos, Um argumento vazio de "" deve ser usado para designar todos os grupos. A

invocação de exemplo
parecido com este:

```
# / Usr / local / nn / lib / nnmaster! Comp rec rec.games.go
```

Note que a ordem é significativa. A especificação do grupo mais à esquerda que corresponda sempre vence. Assim, se

tivéssemos colocado
! Rec.games.go depois *rec*, Todos os artigos deste grupo teria sido, no entanto, rosca.

nn oferece vários métodos para remover artigos expirados a partir do seu banco de dados. A primeira é atualizar o banco de

dados
digitalização dos diretórios newsgroup e descartando as entradas cujos correspondentes artigo tem excedido as suas expi-
ração data. Esta é a operação padrão obtidas por chamar `nnmaster` com o *-E* opção. É razoavelmente
rápida, a menos que você está fazendo isso através de NNTP.

O segundo método se comporta exatamente como um vencimento padrão de execução de `mthreads`, Que remove apenas as

entradas
que se referem os artigos com números abaixo da marca de água baixa na *ativos* arquivo. Ele pode ser ativado usando o *-E* opção.

Finalmente, a terceira estratégia descarta o banco de dados inteiro e relembra todos os artigos. Ele pode ser ativado usando o *-E3* opção.

A lista de grupos a ser vencida é dada pela *-F* opção da mesma forma como descrito acima. No entanto, se você tiver
`nnmaster` como daemon, você deve matá-lo (utilizando *-K*) Antes do vencimento pode ter lugar, e reiniciá-lo com
as opções originais depois. Assim, o comando adequado para executar validade em todos os grupos no primeiro método
é o seguinte:

```
# kF nnmaster ""
# nnmaster-LRC
```

Há muitas mais bandeiras que o ajuste fino do nnDo comportamento. Se você estiver preocupado sobre como remover artigos

ruins ou
montagem digere artigo, leia o `nnmaster` manual de página.

`nnmaster` se baseia em um arquivo chamado *GRUPOS*, Que está localizado na */ Var / nn / lib*. Se ele não existe quando `nnmas-`
`ter` é executado pela primeira vez, ele é criado. Para cada grupo de notícias, ele contém uma linha que começa com o nome do grupo, opcionalmente
seguido por um carimbo de tempo e bandeiras. Você pode editar esses sinalizadores para ativar o comportamento de determinados para o grupo em ques-
ção, mas você não pode alterar a ordem em que os grupos aparecem.[143] Os sinalizadores permitidos e os seus efeitos são detalhadas no `nnmaster` página do manual, também.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

143 Sua ordem tem que concordar com o da inscrição no (binário) *MASTER* arquivo.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Apêndice A

Rede Exemplo: A Cervejaria Virtual

Ao longo deste livro, usamos o exemplo a seguir que é um complexo de pouco menos de Groucho Marx Univer-
diversidade e podem estar mais próximos das tarefas que você vai realmente ocorrer.

A Cervejaria Virtual é uma pequena empresa que fabrica a cerveja, como o nome sugere, virtual. Para gerir o seu negócio mais eficiente, as cervejeiras virtual quer em rede dos seus computadores, que tudo aconteça de ser PCs rodando o mais brilhante e mais brilhante produção do kernel Linux. Figura A.1 shofoi a configuração da rede.

No mesmo piso, em frente ao hall de entrada, há a Adega Virtual, que funciona em estreita colaboração com a cervejaria. A vintners executar uma rede Ethernet do seu próprio. Muito naturalmente, as duas empresas pretende ligar as suas redes, uma vez que
estão operacionais. Como primeiro passo, eles querem criar um host de gateway que encaminha datagramas entre os dois sub-redes. Mais tarde, eles também querem ter uma ligação UUCP para o mundo exterior, através do qual a troca de correio e notícias. No longo prazo, eles também querem estabelecer conexões PPP para se conectar em locais externos e à Internet.

A Cervejaria Virtual ea Adega Virtual cada um tem uma sub-rede classe C de rede de classe B da cervejaria, e porta de entrada para o outro, através do servidor *vlager*, Que também suporta a ligação UUCP. Figura A.2 shofoi a configuração.

Figura A.1: A Cervejaria Virtual e sub-redes virtuais Winery

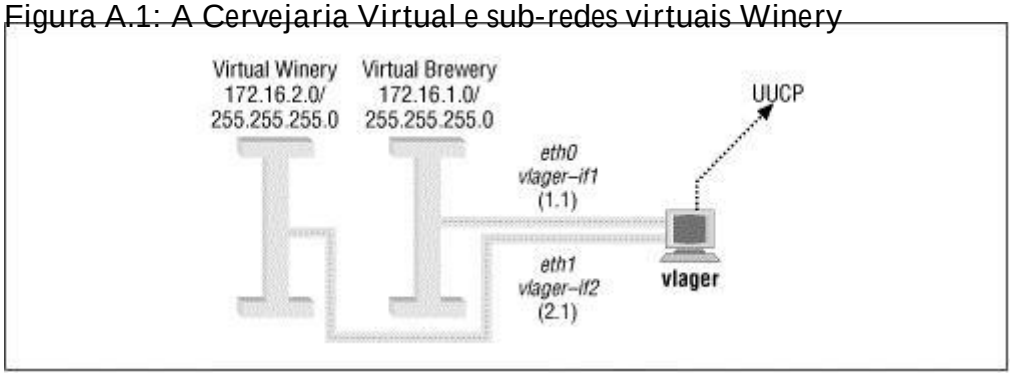
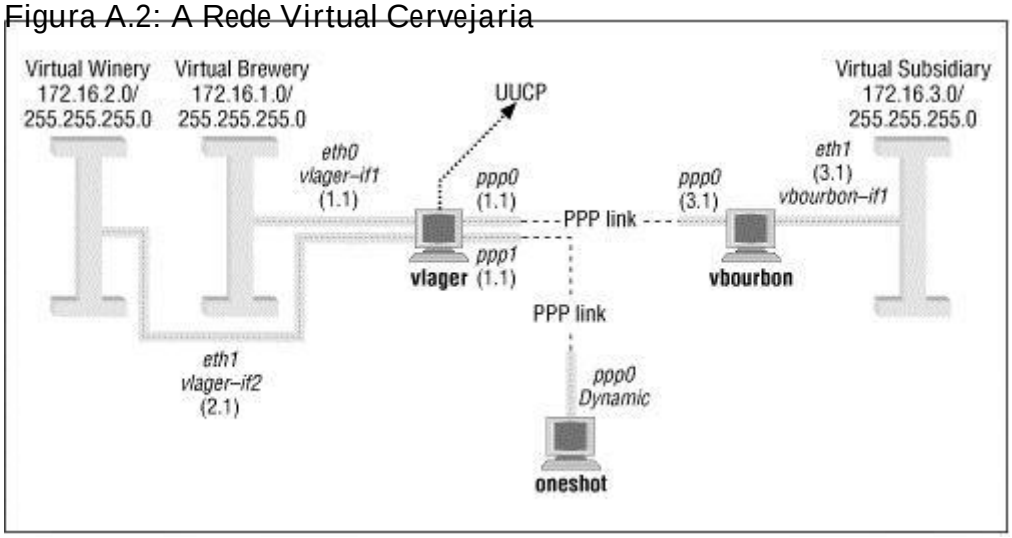


Figura A.2: A Rede Virtual Cervejaria



Conexão da Rede filial virtual

A Cervejaria Virtual cresce e abre uma filial em outra cidade. A subsidiária da funciona uma rede Ethernet de seu próprio uso o número de rede IP *172.16.3.0*, Que é sub-3 da rede de classe B da cervejaria. O anfitrião *vlager* atua como o gateway da rede Cervejaria e apoiará o link PPP; seus pares no novo ramo é chamado *vbourbon* e tem um endereço IP *172.16.3.1*. Esta rede é ilustrado na Figura A.2.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Apêndice B - Útil configurações de cabo

Se quiser ligar dois computadores juntos e você não tem uma rede Ethernet, você precisará de um cabo de modem nulo serial, ou um cabo paralelo PLIP.

Estes cabos podem ser comprados nas prateleiras, mas são muito mais baratas e bastante simples de fazer sozinho.

Um cabo paralelo PLIP

Para fazer um cabo paralelo para usar PLIP, você vai precisar de dois conectores de 25 pinos (chamado DB-25) e um cabo com a pelo menos onze condutores. O cabo não deve ser mais longo do que 15 metros (50 pés). O cabo pode ou não ter um escudo, mas se você está construindo um cabo longo, é provavelmente uma boa idéia ter um.

Se você olhar o conector, você deve ser capaz de ler números minúsculos na base de cada pino - de 1 para o pino na parte superior esquerda (se você segurar o maior voltada para cima) e 25 para o pino no canto inferior direito. Para o cabo da impressora nulo, você tem que ligar os seguintes pinos de ambos os conectores com o outro, como mostrado na Figura B.1.

Todos os pinos restantes permanecem alheios. Se o cabo é blindado, a blindagem deve ser ligada à DB-25's reservatório metálico em apenas *um* finais.

Um cabo de modem nulo serial

Um cabo de modem nulo serial vai funcionar tanto para SLIP e PPP. Novamente, você precisará de dois conectores DB-25. Este vez que o seu cabo requer apenas oito condutores.

Você pode ter visto outros projetos NULL cabo do modem, mas esta permite que você use o controle de fluxo por hardware - que é muito superior ao controle de fluxo XON / XOFF - ou mesmo nenhum. A configuração do maestro é mostrada na Figura B.2:

Novamente, se você tem um escudo, você deve conectá-lo ao primeiro pino de um lado só.

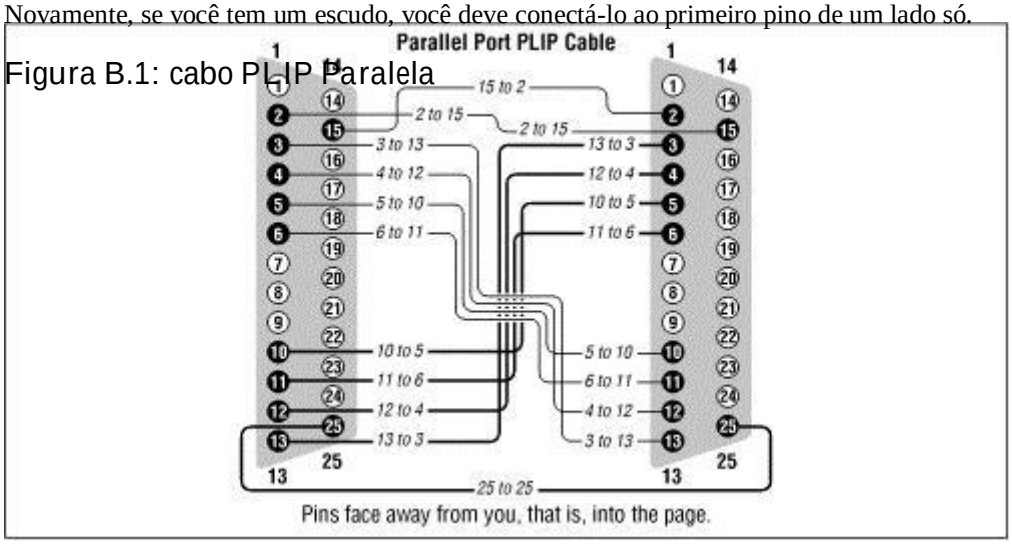
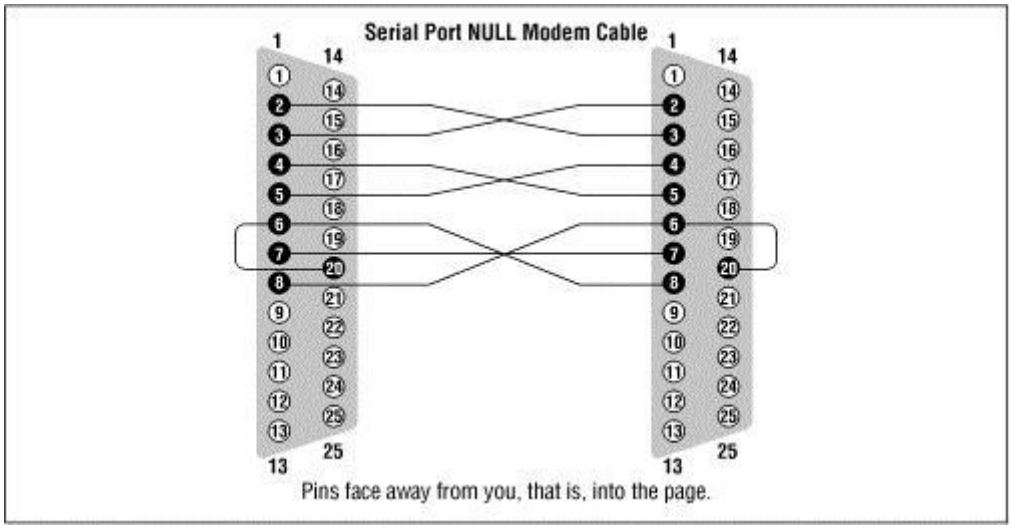


Figura B.1: cabo PLIP Paralela

Figura B.2: cabo de modem nulo serial



PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Anexo C - Informações sobre direitos autorais

Copyright © 1993 Olaf Kirch Copyright © 2000 Copyright Terry Dawson na O'Reilly versão impressa © 2000 O'Reilly & Associates

A versão online deste livro, que no momento da impressão contém exatamente o mesmo texto que o O'Reilly versão impressa, está disponível sob a GNU FDL. Direitos para reimprimir o documento sob a FDL incluem o direito para imprimir e distribuir cópias impressas da versão online. Os direitos de cópia da versão impressa da O'Reilly são reservido. Você pode encontrar a cópia online da licença de http://www.oreilly.com/catalog/linag2/book/copyright.html.O livro está disponível em http://www.linuxdoc.org/LDP/nag/nag.html umdhttp://www.oreilly.com/catalog/linag2/,e pode ser anunciado pelo outros em outras localidades.

É dada permissão para copiar, imprimir, distribuir e modificar o documento on-line sob os termos da GNU Free Documentation License, Versão 1.1 ou qualquer versão posterior publicada pela Free Software Foundation; com as Seções Invariantes sendo os Agradecimentos (no *Prefácio*) E Anexo C, *Administração Linux em rede* *Guia de Tor, Segunda Edição, Informações sobre direitos autorais*.reconhecimentos adicionais podem ser adicionados fora do invariante-
formiga Seção. O Texto de Capa Frontal deve ler-se:

Guia Linux Network Administrator's
por Olaf Kirch e Terry Dawson
Copyright © 1993 Olaf Kirch
Copyright © 2000 Terry Dawson
Direitos autorais na O'Reilly versão impressa © 2000 O'Reilly & Associates

A seguir está uma cópia da GNU Free Documentation License, que também está na http://www.gnu.org/copyleft/fdl.html.

Versão 1.1, Março de 2000
Copyright © 2000 Free Software Foundation, Inc.
59 Temple Place, Suite 330, Boston, MA 02111-1307 EUA
A todos é permitido copiar e distribuir cópias literais
deste documento de licença, mas a mudança não é permitido.

Preâmbulo

O propósito desta Licença é deixar um manual, livro-texto ou outro documento escrito "livre" no sentido do livre-Dom: assegurar a todos a liberdade efetiva de copiar e redistribui-lo, com ou sem modificações, tanto comercialmente ou não. Secundariamente, esta Licença preserva para o autor e editor uma forma de obter crédito pelo seu trabalho, embora não sendo considerados responsáveis por modificações feitas por outros.

Esta licença é um tipo de "copyleft", que significa que derivações do documento precisam ser livres no mesmo sentido. Ela complementa a GNU General Public License, que é um copyleft para livre software.

Nós fizemos esta Licença para que seja usada em manuais para software livre, porque software livre precisa de livre documentação: um programa livre deveria vir com manuais que forneçam as mesmas liberdades que o software faz. Mas esta Licença não está restrita a manuais de software, que pode ser usada para qualquer trabalho em texto, independentemente do sujeito
assunto ou se é publicado como um livro impresso. Nós recomendamos esta Licença principalmente para trabalhos cujo propósito é instrução ou referência.

Aplicabilidade e definições

Esta licença se aplica a qualquer manual ou outro trabalho que contenha um aviso colocado pelo detentor dos direitos autorais

dizendo que
pode ser distribuído sob os termos desta Licença. O "Documento", abaixo, se refere a qualquer tal manual ou trabalho. Qualquer membro do público é um licenciado e é referida como "você".

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Uma "Versão Modificada" do Documento se refere a qualquer trabalho contendo o Documento ou uma parte dele, quer-policial IED na íntegra, ou com modificações e / ou traduzido para outra língua.

Uma "Seção Secundária" é um apêndice ou uma seção inicial do Documento que trata exclusivamente com a relação dos editores ou autores do Documento com o assunto geral do Documento (ou re- questões lated) e não contém nada que possa estar diretamente nesse assunto geral. (Por exemplo, se o Documento é em parte um livro de matemática, uma Seção Secundária pode não explicar nada de matemática). A relação poderia ser uma questão de ligação histórica com o assunto ou com temas relacionados, ou legal, com- posição comercial, filosóficas, éticas ou políticas relacionadas ao mesmo.

As "Seções Invariantes" são certas Seções Secundárias cujos títulos são designados, como sendo de Invariantes Seções, na nota que diz que o Documento é publicado sob esta Licença.

Os "Textos de Capa" são certos trechos curtos de texto que são listados, como Textos de Capa Frontal ou Textos da Quarta

Capa,
na nota que diz que o Documento é publicado sob esta Licença.

Uma cópia "Transparente" do Documento significa uma cópia legível por máquina, representada num formato cuja especi- cação está disponível ao público em geral, cujos conteúdos podem ser visualizados e editados diretamente e sem com editores de texto genéricos ou (para imagens compostas de pixels) programas de pintura genéricos ou (para desenhos) algum amplamente disponíveis editor de desenho, e que é adequado para entrada a formatadores de texto ou para tradução automática para uma variedade de formatos apropriados para inclusão em formatadores de texto. Uma cópia feita em um formato de arquivo Transparente cuja marcação foi projetado para impedir ou desencorajar modificação subseqüente pelos leitores não é Transparente. Uma cópia que não é "Transparente" é chamada "Opaca".

Exemplos de formatos apropriados para cópias Transparentes incluem ASCII simples sem marcações, formato de entrada

Texinfo,
Formato de entrada do LaTeX, SGML ou XML usando uma DTD disponibilizada publicamente, e compatível com os padrões HTML simples projetados para modificação por humanos. Formatos Opacos incluem PostScript, PDF, formatos proprietários que podem ser lidos e editados somente por processadores de texto proprietários, SGML ou XML para os quais o DTD e / ou ferramentas de processamento são Geralmente não estão disponíveis, e HTML gerado automaticamente por alguns processadores de texto para fins de saída representa apenas.

O "Página do Título" significa, para um livro impresso, a própria página do título, além das páginas subseqüentes necessárias

para manter,
de forma legível, o material que esta Licença requer que apareça na página do título. Para trabalhos em formatos que não têm qualquer página de título assim, "Página de Título" significa o texto próximo da aparição mais proeminente do título do trabalho, precedendo o início do corpo do texto.

A cópia fiel

Você pode copiar e distribuir o Documento em qualquer meio, comercialmente ou não, desde que esta Licença, as notas de copyright, ea nota de licença dizendo que esta Licença se aplica ao documento estejam reproduzidas em todas as cópias, e que você não acrescente nenhuma outra condição quaisquer que sejam às desta Licença. Você não pode usar medidas técnicas para obstruir ou controlar a leitura ou ainda cópia das cópias que você fizer ou distribuir. No entanto, você pode aceitar compensação em troca de cópias. Se você distribuir um número suficientemente grande de cópias, você deve também respeitar as condições da seção 3.

Você também pode emprestar cópias, sob as mesmas condições colocadas acima, e você pode exibir cópias publicamente.

Cópia em Quantidade

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Se você publicar cópias impressas do Documento em número maior que 100, ea nota de licença do Documento obrigar Textos de Capa, você precisa incluir as cópias em capas que tragam, clara e legivelmente, todos esses Textos de Capa: Textos de Capa Frontal na capa frontal, e Textos da Quarta Capa na capa. Ambas as capas também claramente e legível, você como o editor dessas cópias. A capa frontal deve apresentar o título completo com todas as palavras do título igualmente proeminentes e visíveis. Você pode adicionar outros materiais às capas. Cópias com mudanças limitadas às capas, tanto quanto estas preservem o título do documento e satisfaçam essas condições, pode ser tratado como cópia exata em outros aspectos.

Se os textos requeridos em qualquer das capas for muito volumoso para caber de forma legível, você deve colocar os primeiros listados (como tantos quantos couberem razoavelmente) na própria capa, e continuar o resto nas páginas adjacentes.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Se você publicar ou distribuir cópias Opacas do Documento em número maior que 100, você deve incluir um legível por máquina cópia Transparente, juntamente com cada cópia Opaca, ou informar em ou com cada cópia Opaca um pub- cou, publica acessível localização rede de computadores contendo uma cópia Transparente completa do Documento, livre de material adicionado, que o público usuário de redes tenha acesso ao download anonimamente, sem custos com padrões públicos de protocolos de rede. Se você usar a última opção, você deve seguir passos razoavelmente prudentes, quando iniciar a distribuição de cópias Opacas em quantidade, para assegurar que esta cópia Transparente vai permanecer assim, aces- veis no local indicado por pelo menos um ano após a última vez que você distribuir uma cópia Opaca (diretamente ou através de seus agentes ou distribuidores) daquela edição para o público.

É solicitado, mas não obrigatório, que você contate os autores do Documento bem antes de redistribuir qualquer grande número de cópias, para dar-lhes uma oportunidade de prover você com uma versão atualizada do Documento.

Modificações

Você pode copiar e distribuir uma Versão Modificada do Documento sob as condições das seções 2 e 3 acima, desde que você publique a Versão Modificada estritamente sob esta Licença, com a Versão Modificada preenchendo o papel do Documento, permitindo assim a distribuição e modificação da Versão Modificada para quem quer possui uma cópia do mesmo. Além disso, você deve fazer estas coisas na Versão Modificada:

1. Use na Página de Título (e nas capas, se alguma) um título distinto daquele do Documento, e de daqueles de versões anteriores (que deveriam, se houvesse algum, estarem listados na seção Histórico do Documento). Você pode usar o mesmo título que uma versão anterior se o editor original daquela versão der permissão.
2. Liste na Página de Título, como autores, uma ou mais pessoas ou entidades responsáveis pela autoria do modificações na Versão Modificada, conjuntamente com pelo menos cinco dos autores principais do Docu- mento (todos seus autores principais, se ele tiver menos que cinco).
3. Estado na Página de Título o nome do editor da Versão Modificada, como o editor.
4. Preserve todas as notas de copyright do documento.
5. Adicionar uma nota de copyright apropriada para suas próprias modificações adjacente às outras notas de copyright.
6. Incluir, imediatamente depois das notas de copyright, uma nota de licença dando ao público permissão para usar o Versão Modificada sob os termos desta Licença, na forma mostrada no Adendo abaixo.
7. Preservar nessa nota de licença as listas completas das Seções Invariantes e os Textos de Capa requeridos dados na aviso de licença do Documento.
8. Incluir uma cópia inalterada desta Licença.
9. Preservar a seção intitulada "História", e seu título, e adicionar à mesma um item dizendo pelo menos o título, ano, novos autores, e editor da Versão Modificada, tal como consta na Página de Título. Se não há a secção en- intitulada "Histórico" no Documento, criar uma dizendo o título, ano, autores, e editor do Docu- mento como dados em sua Página de Título, então adicionar um item descrevendo a Versão Modificada, tal como no anterior- ous sentença.
10. Preservar o local de rede, se algum, dado no Documento para acesso público a uma cópia Transparente o documento, como também os endereços de rede dados no Documento para versões anteriores era baseia. Estes podem ser colocados na seção "Histórico". Você pode omitir uma localização de rede para um trabalho que foi publicado, pelo menos, quatro anos antes do Documento, ou se o editor original da versão- Sion se refere der permissão.
11. Em qualquer seção intitulada "Agradecimentos" ou "Dedicatória", preservar o título da seção e preservar a seção em toda substância e tom de cada um dos agradecimentos e / ou dedicatórias nele indicados.
12. Preservar todas as Seções Invariantes do Documento, inalteradas em seus textos e em seus títulos. Seção números ou equivalentes não são considerados parte dos títulos da seção.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

13. Apague qualquer seção intitulada "Apoio". Tal sessão não pode ser incluído no Rubro-Modificado Sion.

14. Não re-intitular qualquer seção existente como "Apoio" ou entrar em conflito com título de qualquer Seção Invariante.

Se a Versão Modificada incluir novas seções iniciais ou apêndices que se qualifiquem como Seções Secundárias e contenham nenhum material copiado do Documento, você pode optar por designar alguma ou todas aquelas seções como invariável. Para fazer isso, adicione seus títulos à lista de Seções Invariantes na nota da Versão Modificada licença. Estes títulos devem ser distintos de quaisquer outros títulos de seções.

Você pode adicionar uma seção intitulada "Endossos", desde que não contenha nada além de endossos da sua modificação Versão por diversas partes - por exemplo, declarações de revisores ou de que o texto foi aprovado por um organização como a definição oficial de um padrão.

Você pode adicionar uma passagem de até cinco palavras como um Texto de Capa Frontal, e uma passagem de até 25 palavras

como um Back-
Capa de texto, ao final da lista de Textos de Capa na Versão Modificada. Somente uma passagem de Texto de Capa da Frente e uma de Texto de Quarta Capa podem ser adicionados por (ou através de arranjos feitos por) qualquer entidade. Se o Documento já inclui um texto de capa para a mesma capa, adicionado previamente por você ou por arranjo feito pela mesma entidade está agindo em seu nome, você não pode adicionar um outro, mas você pode substituir o antigo, com explícita a permissão do editor anterior que adicionou a passagem antiga.

O autor (es) e editor (es) do Documento não por esta Licença dar permissão para usar seus nomes para publicidade ou para assegurar ou implicar endossamento de qualquer Versão Modificada.

Combinação de documentos

Você pode combinar o Documento com outros documentos publicados sob esta Licença, nos termos definidos no seção 4 acima para versões modificadas, desde que você inclua na combinação todas as Seções Invariantes de todos os documentos originais, sem modificações, e liste todas elas como Seções Invariantes de seu trabalho combinado em sua
nota de licença.

O trabalho combinado somente precisa conter uma cópia desta Licença, e múltiplas Seções Invariantes idênticas podem ser substituídos por um único exemplar. Se houver múltiplas Seções Invariantes com o mesmo nome mas com conteúdos diferentes, faça o título de cada seção único adicionando ao final do mesmo, em parênteses, o nome do original autor ou a editora desta seção, se conhecido, ou então um número único. Faça o mesmo ajuste para a seção títulos na lista de Seções Invariantes na nota de licença do trabalho combinado.

Na combinação, você precisa combinar quaisquer seções intituladas "Histórico" nos vários documentos originais, formando uma seção intitulada "História", da mesma forma combine quaisquer seções intituladas "Agradecimentos", e todas as seções intitulada "Dedicatória". Você deve apagar todas as seções intituladas como "Endosso".

Coleções de Documentos

Você pode fazer uma coleção consistindo do Documento e outros documentos publicados sob esta Licença, e substituir as cópias individuais desta Licença nos vários documentos com uma única cópia incluída na cobrança, desde que você siga as regras desta Licença para cópia exata de cada um dos documentos em todos os outros aspectos.

Você pode extrair um único documento de tal coletânea, e distribuí-lo individualmente sob esta Licença, desde que você insira uma cópia desta Licença no documento extraído, e siga esta Licença em todos os outros re-aspectos relacionados à cópia exata daquele documento.

AGREGAÇÃO COM TRABALHOS INDEPENDENTES

Uma compilação do Documento ou derivados dele com outros documentos separados e independentes ou de obras públicas, ou em um volume de armazenamento ou meio de distribuição, não conta como um todo como uma Versão Modificada do Documento, desde que nenhum copyright de compilação seja reclamado pela compilação. Tal compilação é chamada um agregado ",

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

gate ", e esta Licença não se aplica aos outros trabalhos auto-contidos, assim, compilado com o documento, em conta de terem sido assim compilados, se eles não são trabalhos derivados do Documento.

Se a tampa do requerimento do Texto da seção 3 for aplicável a essas cópias do Documento, então, se o documento é Menos de um quarto de todo o agregado, de Capa do Documento Os textos podem ser colocados em capas que cercam apenas o Documento dentro do agregado. Senão eles precisam aparecer nas capas de todo o agregado.

Tradução

A tradução é considerada como um tipo de modificação, então você pode distribuir traduções do Documento sob o termos do artigo 4. A substituição de Seções Invariantes por traduções requer uma permissão especial da sua cópia titulares de direitos, mas você pode incluir traduções de algumas ou todas as Seções Invariantes em adição à versão original do sões dessas Seções Invariantes. Você pode incluir uma tradução desta Licença desde que você também inclua a versão original em Inglês desta Licença. Em caso de discordância entre a tradução eo original Versão em Inglês desta Licença, a versão original em Inglês prevalecerá.

Rescisão

Você não pode copiar, modificar, sublicenciar ou distribuir o Documento exceto como expressamente previsto no presente Licença. Qualquer outra tentativa de copiar, modificar, sublicenciar ou distribuir o Documento é nula, e será auto-automaticamente rescindirá seus direitos sob esta Licença. No entanto, terceiros que tiverem recebido cópias, ou direitos de você sob esta Licença não terão suas licenças terminadas enquanto tais partes permanecerem em total conformidade.

Futuras revisões desta Licença

A Free Software Foundation pode publicar novas versões revisadas da GNU Free Documentation License partir tempo ao tempo. Estas novas versões serão similares em espírito à versão actual, mas podem diferir em detalhes para endereçar novos problemas ou preocupações. Veja http://www.gnu.org/copyleft/.

Cada versão da Licença é dado um número de versão distinto. Se o Documento especificar que um determinado numerados de versão desta Licença "ou qualquer versão posterior" se aplica a ele, você tem a opção de seguir os termos e condições tanto daquela versão específica, ou de qualquer versão posterior que tenha sido publicada (não como rascunho) pela a Fundação do Software Livre. Se o Documento não especificar um número de versão desta Licença, você pode escolher qualquer versão já publicada (não como rascunho) pela Free Software Foundation.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com

Apêndice D

SAGE: Os Administradores de Sistema

Se você não está recebendo tudo que você precisa de postagem para comp.os.linux .* grupos e documentação de leitura, Talvez seja hora de pensar em se juntar a SAGE, a administradores de sistema Guild, promovido pela USENIX. Os principais objetivo de SAGE é avançar a administração do sistema como uma profissão. SAGE reúne sistema e da rede administradores para promover o desenvolvimento profissional e técnico, compartilhar problemas e soluções, e comunicar com os usuários, gerenciamento e vendedores sobre a administração do sistema.

As actuais iniciativas SAGE incluem:

- Co-patrocínio do grande sucesso Conferências anuais de Administração do Sistema (LISA), com USENIX.
- Editoras `As descrições de cargo para Administradores de Sistemas`, Editado por Tina

Darmohray,

o primeiro de uma série de brochuras muito prático e guias de recursos abrangendo questões de administração do sistema e técnicas.

- Criar um site de arquivamento, *ftp.sage.usenix.org*, Para os documentos das Conferências de Administração do Sistema e documentação relacionada com sysadmin.
- Estabelecer grupos de trabalho em áreas importantes para os administradores do sistema, tais como trabalhos,

publicações,

políticas, distribuição de informação electrónica, educação, fornecedores e padrões.

Para saber mais sobre a Associação e seus USENIX Especial Grupo Técnico, SAGE, em contato com o USENIX Associação escritório em (510) 528-8649 em os EUA, ou pelo e-mail para office@usenix.org. Para receber informações de elec-eletronicamente, entre em contato info@usenix.org. Anual de SAGE adesão é de R $ 25 (você também deve ser um membro de USENIX). Os deputados gozam de assinaturas gratuitas para *login:* e `Sistemas de Computação`, Uma revista trimestral arbitrou-tech técnico periódico; descontos em conferências e simpósios de registo e de poupança nas compras publicação SAGE e outros serviços.

PDF Creator - PDF4Free v2.0 http://www.pdf4free.com